Designing Enforceable Network Contracts

Robert Lychev and Nick Feamster

ABSTRACT

Internet connectivity depends on contractual agreements between cooperating entities, such as administrative domains (AD), where an agreement over a certain level of service is made. Contracts (e.g., SLAs) for providing certain levels of service must be enforceable, and ADs must have an incentive to meet their contractual obligations. Previous work has designed mechanisms for both pricing and network accountability, but no existing work examines contract structures with respect to different accountability frameworks, and how together they may affect an AD's incentives to fulfill contracts. We study how different contract structures—in particular, path-based versus pairwise contracts—affect ADs' incentives to establish contracts (which, in turn, can affect overall connectivity) and, once contracts are established, to forward traffic according accordingly.

This paper presents several contributions. First, we derive sufficient conditions for path-based contract systems and accountability frameworks for entities to have an incentive to forward traffic according to their contracts, provided that all parties involved are rational. Second, we show that for path-based contracts at equilibrium where nodes are encouraged to fulfill their contracts, only a constant amount of monitoring is required for every participant to make a positive profit; this is not the case for pairwise contracts. Third, we show how systems that rely on pairwise contracts are prone to depeering in presence of sufficient supply and demand due to coarse granularity, a contractual failure that systems which rely on path-based contracts are immune to. We propose modifications to pairwise contracts that could prevent such failures. Finally, we present situations of depeering that may be unpreventable due to maliciously behaving parties for both pairwise and path-based contract structures. For such scenarios, we show that while path-based contracts allow the sender of traffic to get reimbursed, this is not guaranteed in pairwise contract systems.

1. Introduction

Connectivity on the Internet has become a contractual business bringing many ADs (contiguous network administered by a single authority [3]) to cooperate via contractual agreements corresponding to desired service levels (e.g., SLA's). In order to prevent ambiguity between cooperating parties, obligations of the parties involved in the contracts must be, first of all, rigorously defined. Also, contracts must be enforceable and provide monetary incentives for partnering ADs to meet contractual promises. Although pricing and incentive mechanisms have been widely studied in the context of network traffic routing (see [1, 2, 11, 14, 15, 17, 21, 28] for some examples), and although much work has been done in the area of network accountability–mechanisms for monitoring ADs' level of service and holding them accountable in case of misbehavior (see [3–5, 12, 16] for some examples)–the research community has not yet scrutinized pricing and incentive mechanisms with respect to different accountability frameworks. We believe this synthesis to be necessary for successful network design because incentive mechanisms by themselves do not guarantee reimbursement in cases of misbehavior while accountability and enforcement by themselves do not guarantee monetary incentives for entities to fulfill contracts in the first place. Below, we first provide background information regarding incentive mechanism design and accountability, followed by a summary of our contributions.

1.0.0.1 Background.

Two main methods for designing incentives are based on either rewarding cooperative nodes [1, 2, 11, 21, 28] or punishing non-cooperative nodes [6, 18, 19]. However, incentive mechanisms by themselves may not guarantee payment to parties who have been denied what they were promised, while punishments by themselves may not provide incentives for participants to engage in relationships. Determining what the price and/or penalty should be has been scrutinized by the research community for various scenarios, but it is not enough to design price and penalty structures without an accountability framework sufficient for proving when an entity deserves to get paid or penalized respectively in the first place.

Enforcement mechanisms of contracts vary depending on the type of accountability scheme used. Modeling the Internet as a graph where nodes represent ADs and edges represent links between ADs, the ideal accountability framework for enforcing contracts must be capable of monitoring quality of service of every node in the network. With node-level accountability, it is straightforward to design incentives so that every node meets contractual obligations: reward those who meet them and penalize those who do not. Unfortunately, no scheme accomplished this design other than assigning a trusted monitor for each node [16], and because of that we mainly focus our study on link-level accountability schemes which must be the next most accurate level of accountability. In case of failure, link-level accountability designs cannot do better than localize a pair of adjacent nodes at least one of which must have not met its promises. Implementing link-level accountability schemes is more practical [3, 5] than node-level accountability schemes, because the former do not require presence of a trusted monitor at each AD. However, designing incentives for the former is more challenging than for the latter, because in link-level settings nothing stops faulty nodes from lying and blaming its neighbors for deviating from contractual obligations and it is not at all clear which node on that link should be pun-

ished and whether any node should be punished at all. Localization of a faulty link alone is not enough by itself because it does not guarantee reimbursement to parties whose traffic suffered poor quality and it may result in depeering as an outcome of a confrontation between the parties sharing that link [24]. Along with network accountability, incentive mechanisms must be used for parties forming contract relationships to have incentive to fulfill their contracts even in cases when fault localization cannot be guaranteed at finer than link-level granularity.

1.0.0.2 Summary of Contributions and Paper Outline.

In this study we define path-based and pairwise contracts and, using node-level and link-level network accountability schemes, we design mechanisms for network participants to cooperate and forward each other's traffic respecting contractual obligations. More specifically,

An important aspect of our model is that contract establishment takes form of market proctored by a single authority, who is a trusted and reliable entity in charge of setting up as well as enforcing contracts between selfish AD's. With this model, we use path-based and pair-wise contracts to study effectiveness of MINT [26] and BGP. An AD can use path-based contracts to purchase a path to destinations of that entity's choice such that each node on that path agrees to forward that entity's bounded-rate traffic to the next node on the path with particular quality. We are motivated by recent progress in the study of path-based connectivity [10, 26, 27] as it promises to provide more options to users regarding level of service and more incentives for networks to cooperate. Any two adjacent ADs can use pairwise contracts to form either peering relations in which they agree to send each other traffic at a bounded rate and forward each other's traffic correctly or client-provider relations where the provider agrees for a fixed price to forward correctly bounded-rate traffic from the client and forward to the client traffic destined to it.

Our main contributions are as follows:

1. present sufficient conditions for path-based contract systems and accountability frameworks that provide incentive for intermediate networks to forward traffic respecting contractual obligations in (Section 3.2.1, Theorem 3.1);

2. present sufficient conditions for path-based and pairwise contract systems for every participant to make a positive profit at equilibrium where participants are discouraged from being faulty while requiring only a constant amount of monitoring in (Section 3.2.2, Theorem 3.2 and Section 3.3.3, Theorem 3.4);

3. when all entities are assumed to be rational, show that pairwise contract systems, unlike path-based ones, suffer from contractual failures—scenarios where available resources are not utilized in the presence sufficient demand caused by depeering—due to coarse granularity of pairwise contracts (Section 3.3) and propose modifications to pairwise contracts for preventing such failures (Section 3.3.3, Lemma 3);

4. discuss malicious behavior, where parties may behave irrationally, that may result in depeering that may be unpreventable in both pairwise and path-based contract systems and show that path-based contracts allow the source of traffic to get reimbursed, something that in general cannot be guaranteed for pairwise contract systems in (Section 4.3).

The rest of this paper is organized as follows. In Section 2 we develop our general model of the Internet, formally define pair-wise and path contracts, and provide formal definitions of successful mechanism design with respect to node-level and link-level accountability settings. Section 3, is devoted to presenting game theoretic analysis and equilibrium evaluation of contract system. In Section 4, we evaluate possible attacks that may occur in contract systems in case of collusion, lack of information, and general distrust. In Section 5 we discuss related work and we finish with a summary of contributions and a discussion of future challenges in Section 6.

2. Model and Contracts

We model the Internet as a graph, where each node represents a separate AD, and each edge represents a bi-directional link. Prior to sending traffic to a destination, the sender node must have first engaged in a contract with at least the next node on the path to that destination during the negotiations stage. We start this section with a general description of our model as a game and its participants as well as notation useful in analyzing games that contract systems may yield. Second, we define two contracts that network participants may engage in to form contract systems. We then present a full description of players' strategies, payoffs, and outcomes. To finalize this section, we present definitions of successful mechanism design for contract systems with respect to node-level accountability without a specific payment structure and link-level accountability for proportional and all-or-nothing payments.

2.1 Game Setup and Notation

Let us refer to any source AD who sends flows of batches of data to various destinations as s. Each such flow $b = b_1, b_2, b_3, ...b_m$ going to some destination d through a set of intermediary forwarding nodes $P_{s\to d} = n_1, n_2, ..., n_\ell$ forms a, possibly dynamic, flow path between s and d, where s is indexed by 0 and d is indexed by $\ell + 1$. s, $n_{1\leq i\leq \ell}$, and d comprise the set of players in our model (see Figure 1). We assume that although every player is selfish, s can be trusted. The players play a finitely repeated game that consists of two stages (we ignore the initial innovation stage presented by Laskowski and Chuang [16] as it is outside the scope of our goals of providing incentives and enforcement for forwarding traffic):

1. **Negotiations Stage**, where all participants of the game establish contracts;

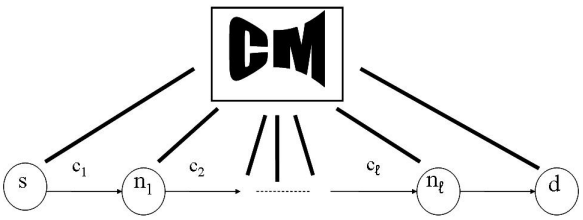

Figure 1: Basic game set up. Contract Mediator (CM) is in charge of setting up flow paths and enforcing contracts. Thick lines represent trusted channels.

2. **Forwarding Stage**, which consists of a finite number of rounds such that per round each participant is allowed to send an amount of traffic to an adjacent participant no larger than the capacity of the link between them, and, as long as this stage is not over, any batch of packets received at round k, unless it reached its destination, must be forwarded to the next node at round $k+1$.

We assume that s sends batches successively beginning at the first round of the forwarding stage and that the length of the forwarding stage permits the last batch in b to reach d. The game is administered by a trusted party, the CM, who is in charge of setting up as well as enforcing contracts between participants during the negotiations and forwarding stages respectively. The CM should ensure correct execution of incentive mechanisms and guarantee accountability even in cases with multiple independent adversaries. We assume that every network participant has access to a trusted and reliable out-of-band communication channel with the CM. Prior to the forwarding stage, s must have established a business relationship with at least n_1, otherwise s will not be able to send anything to d. All of notation for parameters we use to represent and analyze contract systems is summarized in Tables 1- 2.

We extend formal notation used to express quality of service introduced in [16]. Let us represent network flow quality by a finite dimensional vector space Q, where each dimension represents a distinct network flow characteristic such as transmission rate, expected packet delay, and loss probability. We define a binary operator, $* : Q \times Q \rightarrow Q$, that is used to combine elements of Q. For each component of $\mathbf{q} \in Q$, $*$ operator represents an operation appropriate to the network flow characteristic of that component. For instance, for characteristics of maximum transmission rate (bandwidth), expected packet delay, and throughput fraction, $*$ operator represents the min function, addition, and multiplication respectively. We can associate with each node n_i and each path $P_{s\rightarrow d} = (n_1, n_2, ..., n_\ell)$ vectors $\mathbf{q}_i \in Q$ and $\mathbf{q}_{n_1} * \mathbf{q}_{n_2} * ... * \mathbf{q}_{n_\ell} = \mathbf{q}_{P_{s\rightarrow d}} \in Q$ respectively. Functionality of the $*$ operator can be used by the CM to check the aggregate quality of any path throughout the game. Operator * for elements of $Q \times \Psi$ is defined as follows: $\langle q, \psi\rangle^* \langle \tilde{q}, \tilde{\psi}\rangle = \langle q * \tilde{q}, \psi || \tilde{\psi}\rangle, \forall\ q, \tilde{q} \in Q$ and $\forall\ \psi, \tilde{\psi} \in \Psi$, where $||$ is the operation of concatenation. Here Ψ is the space of all possible proofs that could support any element of Q. Functionality of the * operator can be used by the CM to provably verify the aggregate quality of any path during the forwarding stage. We define a function $u : Q \times \Psi \rightarrow \mathbb{R}$ that can be used by the CM to reduce the evaluation of the quality of a path to an analysis of a single real.

Notation	Explanation
	Basic Setup (Section 2.1)
CM	– contract mediator
s	– source of traffic
d	– destination of traffic
$P_{s\rightarrow d}$	– flow path from s to d
n_i	– i^{th} forwarding node on $P_{s\rightarrow d}$
ℓ	– total number of forwarding nodes on $P_{s\rightarrow d}$
b	– flow of batches of data
m	– the number of batches that comprise b
b_j	– j^{th} batch in b $1 \leq j \leq m$
	Used in Path-Segment and Pairwise-Exchange Contracts
T	– contract duration (measured in rounds)
N/N_i	– max batch size in general/node/neighbor i has bandwidth for per round
c_i	– batch bandwidth cost of node/neighbor i for forwarding
C_i	– monetary commitment to node/neighbor i for bandwidth over T
$\mathbf{p}_i$	– penalty specification for node/neighbor i for not meeting contractual obligations wrt a single batch
$PrvsNd_i$	– required next up-stream node to n_i on the flow path
$NxtNd_i$	– required next down-stream node to n_i on the flow path
Ψ_i	– specification on how n_i must form proofs of quality of service
ν_i	– frequency n_i of providing proofs for fulfilling contracts
u_i	– evaluator function of overall QoS of node/neighbor i
u_{min_i}	– minimum quality of network service of node/neighbor i
	Used in Pairwise-Exchange Contracts Only
$e_{j\in\{0,1\}}$	– j^{th} neighbor
$Tbl_{j\in\{0,1\}}$	– e_j's routing table that defines how to forward $e_{\bar{j}}$'s traffic
	More Negotiations Stage Params (Section 2.3.1)
t_i	min parts of a batch in b n_i is required to forward
t	min parts of a batch in b that must reach d for s to gain utility
u_i	utility s gains when at least t parts of b_i reach d uncorrupted
p_{i_a}	n_i's penalty when unable to prove meeting t_i
p_{i_b}	n_i's penalty when unable to prove that n_{i-1} does not meet t_{i-1}

Table 1: Basic setup parameters (Section 2.1), parameters important for the negotiation of Path-Segment and Pairwise-Exchange contracts introduced in Sections 2.2.1 and 2.2.2 respectively, and additional negotiation-strategy parameters introduced in Section 2.3.1.

We elaborate on this notation with respect to our model for some forwarding node n_i. The duration of contracts T is defined by the total number of rounds $m + \ell + 1$, and the frequency ν_i is once per round. Ψ_i should be provided as specified by ν_i (once per round), however, participants could agree to provide proofs of service for smaller values than the whole batch so that in case of partial failures only a fraction of a batch may require retransmission. We take the allowed delay across all the contracts to be the time that lapses between rounds (assuming time synchronization), and we assume that the size of every batch in b is the same, is measured in packets, and is subject to negotiation during the competition stage such that it is the batch size, $|b_j| = N\ \forall\ 1 \leq j \leq m$, that determines the maximum desired rate of transmission, where the unit of time is a single round. Since every forwarding node n_i might be penalized the same for forwarding less than t_i packets, where $N - t_i$ is the maximum allowed batch part loss agreed upon in advance, of a message as for delaying more than $N - t_i$ packets of a message for more than one round, there is no incentive for any participant to forward traffic delayed for more than one round; with this in mind, for each round and for each batch, quality $\mathbf{q}_i$ represents the amount of parts of that mes-

Notation	Explanation
	Forwarding Stage Params (Section 2.3.1)
σ_0	– probability of s sending a batch in b
$\sigma_{1\leq i\leq \ell}(\varphi)$	– probability that n_i forwards φ parts of a batch in b
φ_i	– number of parts of a batch in b n_i forwards correctly
$\lambda_{i_a}(\varphi_i)$	– probability n_i claims to have sent φ_i parts to n_{i+1}
$\lambda_{i_b}(\varphi_{i-1})$	– probability n_i claims that n_{i-1} sent φ_{i-1} parts to n_i
	Profit-Related Params (Sections 2.3.2- 2.3.3)
f_i	– marginal cost of forwarding a batch of n_i
ϵ_x	– minimum profit entity x is willing to settle for
π_x	– profit of entity x

Table 2: Parameters for forwarding-stage strategies and profits of games contractual agreements yield, detailed in Sections 2.3.1 - 2.3.3.

sage participant n_i forwards during that round, $u_i(\mathbf{q}_i, \psi_i)$ evaluates to 1 if t_i is met (provided that ψ_i checks out) and 0 otherwise, and u_{min_i} is always 1.

2.2 Contract Setup

A contract is a set of agreements that must be established during the negotiations stage. First, we describe the Path-Segment contract, which is appropriate in relationships when a source s wants to ensure that a forwarding node forwards s's traffic with particular quality along an established path. Second, we describe the Pairwise-Exchange contract, which is appropriate to situations when two adjacent nodes want to agree on the uses of the link that connects them. The pairwise contract can be used to form contracts prevalent in the current day Internet, namely client-service-provider contract and peering contract. Although path contracts do not address quality of a node's incoming traffic, assuming that every node, prior to sending any traffic, must have engaged in a contract with respect to all of its outgoing traffic, pairwise contract do address quality of incoming traffic for client-service-provider and peering variations.

2.2.1 *Path-Segment Contract*

DEFINITION **Path-Segment Contract** A *Path-Segment Contract* is an agreement between a source s and any forwarding node $n_i \in P_{s\to d}$ on parameters as specified in in Table 1 above. ■

We elaborate on some of the notation relevant to this contract that is summarized in Table 1. ν_i is the frequency with which n_i must measure and provide $\langle \mathbf{q}_{n_i}, \psi_{n_i} \rangle$ to the CM (i.e. ν_i divides T into rounds based on criteria such as time or content volume), Ψ_i defines the appropriate ψ_{n_i} for each possible $\mathbf{q}_{n_i}$, N_i defines the volume of traffic measured in data parts (assumed to be of the same size for every participant) per time period specified by ν_i, C_i defines the minimum amount s must pay to n_i over the duration of the contract, $\mathbf{p}_i$ defines the various penalties for n_i to pay s in case of violation of various contractual agreements such as ν_i and/or Ψ_i and/or $NxtNd_i$, and/or u_{min_i}. Over the course of the contract n_i must pay according to $\mathbf{p}_i$ to s for every $\mathbf{q}^j_{n_i}$ that it provides if $u_i(\langle \mathbf{q}^j_{n_i}, \psi_{n_i} \rangle) < u_{min_i}$, and s must pay c_i to n_i when $u_i(\langle \mathbf{q}^j_{n_i}, \psi_{n_i} \rangle) \geq u_{min_i}$ for any outgoing flow of s's traffic for every round j.

MINT contracts [26] is an example of contracts that Path-Segment contracts can model. During the negotiation stage, the CM collects network advertisements from different forwarding nodes and path requests from different sources. Forwarding node's advertisements come in the form of offers consisting of the quality of a particular network segment being offered and the price the advertiser of that segment is willing to accept for that segment at that quality. A source's requests come in the form of bids consisting of the source and the destination of a desired path, quality of that path, and the price that source is willing to pay for a path at that quality. Path quality can be measured in terms of available bandwidth and maximum packet delay and/or max packet loss, which we model with maximum allowed parts N and minimum forwarded parts $t_{1\leq i\leq \ell}$ respectively (see Sections 2.1). When collection of advertised path segments forms a path with the quality satisfies the source, the CM facilitates the establishment of Path-Segment contracts between that source and each forwarding node on the desired path. Source's bid can be satisfied only if offers with sufficient quality are available at a price not greater than the bid.

During the forwarding stage, the CM collects proofs of and complaints about quality of service from different forwarding nodes and sources, respectively. As a response to a source's complaint, the CM is responsible for administering punishment when a forwarding node is not able to provide proof of meeting contractual obligations. The CM is also responsible ensuring that every forwarding node gets paid respecting the contracts.

2.2.2 *Pairwise-Exchange Contract*

DEFINITION **Pairwise-Exchange Contract** A *Pairwise-Exchange Contract* is an agreement between a pair of neighbors (e_1, e_2) to exchange traffic via the link that connects them respecting the parameters as specified in Table 1. ■

All the parameters in this contract are semantically identical to those defined in the Path-Segment contract except for (Tbl_1, Tbl_2), that specifies routing tables that define how e_1 must forward e_2's traffic and vice versa based on that traffic's destination while respecting some notion of route optimality predefined by the CM. Since this contract defines quality of service of traffic flowing in both directions between e_1 and e_2 we use subscripts to identify each parameter with its party, e.g., c_1 is bandwidth cost of e_1 while C_2 is e_1's commitment to e_2's bandwidth.

During the negotiation stage, the CM establishes Tbl for each node, proctors negotiation, and records Pairwise-Exchange contracts between adjacent pairs of nodes who engage in such contracts. The CM updates Tbl over the course of the contracts when necessary. Because the CM is not responsible for monitoring overall path $P_{s\to d}$ quality for any s and d, no source has control over the quality of any path during the negotiations stage of the game. For any s and d the quality of $P_{s\to d}$ is defined by Tbl and Pairwise-Exchange contracts of each node and each edge on the path respectively, and this quality may change over the course of the forwarding stage of the game. During the forwarding stage, responsibilities of the CM are analogous to those for Path-Segment contracts.

Adjacent nodes can peer with each other by establishing symmetric Pairwise-Exchange contracts. Also, stub-networks and end hosts can form customer-provider types of relationships with provider ADs by forming asymmetric Pairwise-Exchange contracts.

2.3 Strategies, Utilities, and Outcomes

In this section, we will mainly focus on describing strategies, utilities, and outcomes of players for the link-level accountability setting. We will also comment on how our description could be extended to the node-level accountability setting.

2.3.1 *Strategies*

In this subsection we will define strategies of different player for the negotiation and forwarding stages.

Negotiation Stage Strategies

During the negotiations stage, the strategy space of a forwarding node n_i on $P_{s\to d}$ consists of negotiating all possible values of all parameters included in the contracts. All notation required to follow negotiation-stage strategies is presented in Table 1. We focus on the most important parameters c_i, C_i, t_i and p_i. For link-level accountability settings we define **p** as penalties $\langle p_{i_a}, p_{i_b}\rangle$ that n_i suffers when unable to prove either that n_i met t_i or that n_{i-1} did not meet t_{i-1} respectively.

For node-level accountability, **p** is a single value corresponding to p_{i_a} in link-level accountability settings. The following is the *strategy space* of a forwarding node $n_{1\le i\le \ell} \in P_{s\to d}$ when negotiating with the source s or any other forwarding node in $P_{s\to d}$:

1. **adjust the price** of an advertised segment by:
   (a) adjusting bandwidth cost c_i while keeping advertised bandwidth $|b_{1\le j\le m}| = N$ and threshold t_i constant or
   (b) adjusting N while keeping c_i and t_i constant or
   (c) adjusting t_i while keeping N_i and c_i constant;
2. **adjust commitment** C_i for bandwidth N_i;
3. **adjust penalties** p_{i_a} and p_{i_b}.

The CM does not conclude the negotiations until purchasers of bandwidth from n_i commit by providing the CM with C_i. The CM should check and distribute these commitments to sellers of bandwidth prior to the forwarding stage.

Forwarding Stage Strategies

For each batch in b, each forwarding node n_i in $P_{s\to d}$ has an option of forwarding a number φ_i of parts of that batch to the next forwarding node in $P_{s\to d}$ with probability given by a discrete random variable σ_i. The source s sends each batch in b with probability σ_0, and we assume that this probability is identical and independent for each batch. For every batch b_j, $\forall\ 1 \le j \le m$, s gains utility u_j if some minimum number of parts t of b_j make it to d and 0 otherwise. If less than t parts of a batch reach d, then the source s may gain utility via a reimbursement from entities that did not fulfil their contracts. The thresholds are set up such that for any $i < j,\ t_i \ge t_j,\ t_0 = N$ and $t_\ell = t$. No node n_i is responsible for forwarding a batch in b if it can show that it received less than t_{i-1} parts of that batch the previous round. The following assumptions are important for analysis contract systems.

ASSUMPTION 1 (UNINTENTIONAL DROPS). *The difference between thresholds t_i and t_{i+1} of adjacent forwarding nodes n_i and n_{i+1} reflects the amount of parts n_{i+1} may unintentionally drop in the worst case congestion.*

ASSUMPTION 2 (INDEPENDENCE). *Any number of parts that a node unintentionally drops due to congestion is independent of every other number of parts that node may unintentionally drop due to congestion.*

ASSUMPTION 3 (PERFECT LAST LINK). *The destination always receives everything that the last node n_ℓ in $P_{s\to d}$ forwards to d.*

While the unintentional drop assumption allows us to assume that no more than $N - t$ parts of any batch in b get unintentionally dropped along $P_{s\to d}$, the independence assumption allows us to express probability of a union of part-drop events as a sum of probabilities of those events. Lastly, we assume that the link between the destination and the last node n_ℓ is perfect, and this assumption allows us to simplify profit analysis of participants presented in Section 3.

In the link-level setting, when a node n_i does not forward at least t_i parts of a batch in b, it has the option of lying by claiming receipt and shipment of $\varphi_{i-1} < t_i$ and $\varphi_i \ge t_i$ parts of that batch with probability $\lambda_{i_b}(\varphi_{i-1} < t_i)$ and $\lambda_{i_a}(\varphi_i \ge t_i)$ respectively. For our study, we assume the following rule:

DEFINITION **Claiming Shipment Rule** At no round is a forwarding node $n_{1\le i\le \ell}$ allowed to claim that it meets t_i for any batch $b_j \in b$ unless it proves receipt of at least t_{i-1} parts of b_j from n_{i-1} the previous round. ■

This rule is useful in analyzing incentives in link-level accountability settings as it provides incentive for forwarding nodes to issue acknowledgments of receipt. For n_i, the value of $\lambda_{(i+1)_b}(\varphi_i)$ signifies the probability with which n_{i+1} acknowledges the receipt of φ_i parts from n_i.

For every round, the *strategy space* for a forwarding node $n_{1\le i\le \ell}$ in $P_{s\to d}$ for every t_{i-1} parts of every batch in b that n_i receives from n_{i-1} is:

1. **Comply** by forwarding $\varphi_i \ge t_i$ parts of that batch to the next node in $P_{s\to d}$, thereby acknowledging receipt of at least t_{i-1} parts of that batch from n_{i-1} the previous round;
2. **Trick** by forwarding $t \le \varphi_i \le t_i$ parts of that batch to the next node in $P_{s\to d}$ (only applicable to link-level settings with all-or-nothing payments);
3. **Cheat** by dropping the batch entirely and, exclusively
   (a) either lie about not receiving at least t_{i-1} parts of that batch
   (b) or lie about forwarding at least t_i parts of that batch to the next node in $P_{s\to d}$ (this requires from

n_i proof of receipt of at least t_{i-1} parts of that batch from n_{i-1} the previous round).

Note that for link-level settings with proportional payments, if a node does not meet its threshold, then it is not going to forward anything to avoid extra forwarding costs since it in this case it will get penalized anyway.

The strategy spaces of the source node s for each batch in b and destination node d for each batch it receives from n_ℓ are respectively:

(1) $\sigma_0 = 1$: to send the whole batch along $P_{s\to d}$;

(2) $\sigma_0 = 0$: to send no part of the batch along $P_{s\to d}$;

and

(1) to confirm receipt of φ_ℓ parts of that batch;

(2) to lie about receiving φ_ℓ parts of that batch.

Since in node-level accountability settings no node can lie about its performance, a forwarding node's strategy space in this case is either to meet its threshold or to drop the message entirely.

2.3.2 *Utilities*

All material utility is gained and/or lost during the forwarding stage of the game. Because bandwidth is committed to its purchasers via the CM for the entire duration of the forwarding stage, payments and reimbursements in forms of penalties are proctored by the CM for every participant of the game per every round where applicable. Every node $n_{1\le i\le \ell}$ experiences a marginal cost of $\frac{f_i}{N}$ for forwarding a single part of any batch in b. Below we summarize profit of a forwarding node $n_{1\le i\le \ell}$, for every batch in b, for link-level accountability settings with payments proportional to the amount of parts forwarded and all-or-nothing payments respectively. Note that for the latter setting punishment is administered only when $\varphi_\ell < t$.

Payments Proportional to φ_i:

1. $+\frac{\varphi_i}{N}(c_i - f_i)$ for forwarding $\varphi_i \ge t_i$ of that batch and able to prove shipment of φ_i packets of that batch;
2. $-(\frac{\varphi_i}{N} f_i + p_{i_a})$ for forwarding $\varphi_i \ge t_i$ parts of that batch when unable to prove shipment of φ_i packets of that batch;
3. $-p_{i_b}$ for dropping the batch entirely and lying about not receiving it or lying about sending it at least t_i parts of that batch to n_{i+1} while unable to prove receipt of at least t_{i-1} parts of that batch the previous round from n_{i-1};
4. $-p_{i_a}$ for dropping the batch entirely and lying about sending it at least t_i parts of that batch to n_{i+1} and able to prove receipt of at least t_{i-1} parts of that batch the previous round from n_{i-1}
5. $-p_{i_b}$ when unable to prove lack of shipment on the part of n_{i-1} of at least t_{i-1} the previous round.

All-or-Nothing Payments:

1. $+(\frac{t_i}{N} c_i - \frac{\varphi_i}{N} f_i)$ for forwarding φ_i packets of that batch when either able to prove shipment of at least t_i parts of that batch to n_{i+1} or $\varphi_\ell \ge t$;

2-5. are the same as in settings with payments proportional to the amount of parts forwarded with the additional requirement that φ_ℓ must be less than t.

For node-level settings, for every batch in b that any participant n_i sees, provided that it receives at least t_{i-1} packets of that message the previous round from n_{i-1}, n_i makes $\frac{\varphi_i}{N}(c_i - f_i)$ and for $c_i - \frac{\varphi_i}{N} f_i$ for forwarding $\varphi_i \ge t_i$ parts of that batch for proportional and all-or-nothing payments respectively. If $\varphi_i < t_i$, then n_i gets penalized p_i.

For both node-level and link-level accountability settings alike, source's utility is the sum of utilities of batches that make it to d containing at least t parts. Destination does not have any utility in this game unless in the node-level accountability settings, but, in the link-level accountability settings, if it is suspected that $\varphi_\ell \ge t$ but d intentionally does not acknowledge receipt of at least t parts of a batch in b from n_ℓ, d will be penalized $p_{(\ell+1)_2}$.

2.3.3 *Outcomes*

The outcome of the negotiation state is a vector of quadruples $\langle \{c_1, C_1, t_1, \mathbf{p}_1\}, \{c_2, C_2, t_2, \mathbf{p}_2\}, \dots, \{c_n, C_n, t_n, \mathbf{p}_n\}\rangle$ that specifies for every forwarding node $n_i \in P_{s\to d}$ bandwidth cost of forwarding a single batch, overall bandwidth commitment, minimum forward threshold and penalties for not meeting contractual obligations. The outcome of the forwarding stage is a vector $\langle \langle \varphi_{1_1}, \varphi_{1_2}, \dots, \varphi_{1_m}\rangle, \langle \varphi_{2_1}, \varphi_{2_2}, \dots, \varphi_{2_m}\rangle, \dots, \langle \varphi_{\ell_1}, \varphi_{\ell_2}, \dots, \varphi_{\ell_m}\rangle, \rangle$ that summarizes forwarding action φ_{i_j} of $n_{1\le i\le \ell}$ with respect to each batch $b_j \in b$ and a vector $\langle \pi_s, \pi_{n_1}, \pi_{n_2}, \dots, \pi_{n_\ell}, \pi_d\rangle$ that summarizes profit of each entity in $P_{s\to d}$.

The desirable outcome is an equilibrium at which traffic is forwarded respecting the thresholds and each entity makes at least its minimum settlement–minimum profit an entity is willing to settle for. More concretely, the desirable outcome is when $\varphi_{i_j} \ge t_i \ \forall\ 1 \le j \le m, \forall\ 1 \le i \le \ell, \pi_{n_i} > \epsilon_{n_i} \ \forall\ 0 \le i \le \ell + 1$ and no entity in $P_{s\to d}$ can gain by unilateral deviation.

2.4 Successful Mechanism Design

For these definitions and analysis of contract systems with respect to these definitions we assume that no node has hidden utility for doing malice that cannot be accounted for with penalties.

DEFINITION **Faulty** We say that a forwarding node is faulty if it fails to meet at least one of its contractual obligations. ■

DEFINITION **Success, Node-level** A mechanism design for a contract system that forms a path $P_{s\to d}$ is successful with **Node-Level Accountability**, when all of the following are true:

1. During Negotiations Stage: The CM can guarantee that for no participant is it profitable to advertise bandwidth it does not have;

2. During Forwarding Stage: for every round over the duration T of the contract, for every participant A, for every participant B who has contractual obligations to A, the CM can guarantee that B gets paid at least C from A and A gets reimbursed from B when B is faulty;

3. At Equilibrium: The CM can guarantee that if there exists an available path $P_{s\to d}$ such that s's overall utility obtained when its traffic is treated with particular quality of service along $P_{s\to d}$ is no lower than s's marginal costs for using $P_{s\to d}$ in addition to s's minimum settlement ϵ_s, then there exists an equilibrium such that

   (a) during the negotiations stage, the CM is capable of constructing a contract system forming a path $P_{s\to d}$ that satisfies that particular quality of service and ensures that minimum settlement of every forwarding node on $P_{s\to d}$ is met

   (b) during the forwarding stage, for no node on $P_{s\to d}$ is it profitable to be faulty with respect to s's traffic.

■

Node-level accountability may be very appealing as it guarantees that any source will always be able to detect the node(s) responsible for failure(s) for Path-Segment as well as Pairwise-Exchange contracts. However, guaranteeing success in such a setting presents an impractical task in the context of real-world networks because it is hard to provably localize the faulty node unless there is a mechanism capable of providing proofs regarding the quality of service of each forwarding node in the system. As we have already mentioned, having a trusted monitor with ability to observe the quality of every node, as proposed in [16], will solve the problem of network accountability trivially, but such solution is impractical. We describe an idea of approaching this issue more efficiently in our technical report [29]. It must be noted that none of the network accountability frameworks proposed in [3, 5, 16] satisfies our definition of success with node-level accountability for Path-Segment contract systems because neither scheme guarantees localization of the exact faulty forwarding node(s) in the network with multiple independent adversaries. Localization of a faulty link – a pair of neighboring entities one of which must be the faulty one – is the most accurate result that solutions proposed in [3, 5] can provide.

DEFINITION **Success, Link-level, Proportional** A mechanism design for a contract system that forms a path $P_{s\to d}$ is successful with **Link-Level Accountability and Payments Proportional to the Amount of Parts Forwarded**, when all of the following are true.

1. During Negotiations Stage: Same as in Definition 2.4;

2. During Forwarding Stage: for every round over the duration T of the contract, for every participant A $\in P_{s\to d}$, for every participant B $\in P_{s\to d}$ who has contractual obligations to A: the CM can guarantee that B gets paid at least C from A, B gets paid the proportion of c that respects the amount of parts that it forwarded when it is not faulty in addition to C, and A gets reimbursed from B and/or B's adjacent neighbor when either B or that adjacent neighbor is faulty;

3. At Equilibrium: Same as in node-level success definition. ■

DEFINITION **Success, Link-level, All-or-nothing** A mechanism design for a contract system that forms a path $P_{s\to d}$ is successful with **Link-Level Accountability and All-or-Nothing Payments**, when all of the following are true.

1. During Negotiations Stage: Same as in Definition 2.4.

2. During Forwarding Stage: for every round over the duration T of the contract, for every participant A $\in P_{s\to d}$, for every B $\in P_{s\to d}$ who has contractual obligations to A, the CM can guarantee that B gets paid at least C from A, A gets reimbursed from B and/or Bs adjacent neighbor when the overall quality of $P_{s\to d}$ does not meet the overall quality of service aggregated over every B with contractual obligations to A and either B or that adjacent neighbor is faulty;

3. At Equilibrium: Same as in node-level success definition with the addition that at equilibrium during the forwarding stage the CM should not have to check more than a constant number of proofs of quality of service. ■

While the first definition of successful mechanism design for contract systems with link-level accountability requires that each forwarding node meets contractual obligations, the second definition of successful mechanism design for contract systems with link-level accountability only requires that the desired overall path quality is met. The purpose to have proportional payments is to provide each node with incentive to forward as much as possible, thereby increasing the chances that the overall path quality is met. However, a mechanism that satisfies the second definition is more practical than a mechanism that can satisfy only the first one from a computational point of view because with the second definition, as long as the desired overall path quality is met, there is no need to check quality of service of each node on the path at equilibrium. The definition of successful mechanism design for contract systems with node-level accountability does not assume any payment structure, but it can be easily extended to settings where payments are proportional to the amount of parts forwarded as well as all-or-nothing payments analogously to definitions of successful mechanism design for contract systems with node-level accountability.

Neither of the weak settings is as appealing as the strong setting because in former settings a source cannot localize the exact faulty node. Due to this, no source is able to penalize the faulty node unless one is willing to punish both nodes sharing the faulty edge, which does not suit Pairwise-Exchange contract establishments at all. Although in such

settings every source is guaranteed at least not to waste funds on faulty nodes, the fact that a source may potentially punish an innocent forwarding node that just happened to be adjacent to a faulty node along the path of that source's traffic is an important weakness that may discourage some parties from establishing contracts with that source in the first place. Also, in Pairwise-Exchange establishments even if an emitter's traffic is completely ignored by its receiver, the emitter still must pay that receiver C because the emitter cannot prove anything about what it sent. However, the weak settings are more applicable to real world networks than the strong setting, and practical schemes for localization of faulty edges have already been proposed [3, 5] for networks with a single adversary.

3. Contract System Analysis

In this section, we show how different contract systems perform with respect to success definitions described in Section 2.4 for contract systems with link-level accountability for proportional and all-or-nothing payments. First, we analyze honesty during the negotiations stage, followed by accountability during the forwarding stage for path-based as well as pairwise contract systems. We then continue with a formal treatment of participant profit model, state conditions sufficient for Path-Segment contracts satisfy both link-level success definitions, show how Pairwise-Exchange contract systems satisfy neither of link-level success definitions and propose modifications to Pairwise-Exchange contracts that could make systems based on the latter meet link-level success definitions. For all of our analysis we assume that bandwidth may be purchased in any denomination. Analysis of Path-Segment contract systems with node-level accountability is presented in our technical report [29].

3.1 Honesty and Accountability

The negotiation stage is not over until an equilibrium—a point where no player gains by adjusting any of the parameters for any of the contracts that player is engaged in—-is reached. The challenge of preventing players from lying about true costs of their goods has already been addressed [2,9,11,20], so we do not focus on this issue. To discourage players from advertising bandwidth they do not have during the negotiations stage the CM must ensure that the gains a forwarding node obtains from advertising bandwidth it does not have must be less than the penalties that node will suffer upon failing to meet contractual obligations. In Sections 3.2 and 3.3, we show that this is a necessary condition for the source to send any traffic, and in Section 4.2 we present mechanisms for specifying the penalties to ensure that nodes are discouraged from dropping traffic and making false advertisements (see 4.1 for an attack).

Our study does not focus on the implementation details of various accountability frameworks. We assume that node-level and link-level accountability frameworks that function correctly in the presence of multiple independent adversaries exist. Assuming only a single adversary, as is done in [5,16], is a weakness because every node on a path, being selfish and rational, can be a potential adversary. Our analysis mostly focuses on link-level accountability settings, and our mechanism for proving an entity's quality of service are based primarily on that entity obtaining proof of receipt from the next entity down the stream. The proofs of receipt must be unforgeable (see our technical report for details [29]). Proofs of receipt can be collected by the CM via an out-of-band trusted channel that we assume every participant has with the CM.

3.2 Success of Path-Segment Contracts

In this section we analyze Path-Segment contract systems with respect to link-level accountability for two types of payments: proportional and all-or-nothing. We show that Path-Segment systems meet both link-level success definitions. The proofs of Lemmas 1 and 2 and Theorems 3.1 and 3.2 are presented in our technical report [29].

3.2.1 *Proportional Payments*

When every forwarding node is encouraged to forward as much traffic as possible, the probability of at least t parts of each batch in b to reach d is higher. This is the motivation for studying systems with proportional payments, where the more a forwarding node forwards the more it gets paid. To show that Path-Segment contract systems satisfy definition of successful mechanism design with link-level accountability and proportional payments, we are going to analyze the expected profit of forwarding nodes and the source to find scenarios where s's traffic reaches d, and s and every forwarding node make positive profit.

When an agreement is reached in the negotiations stage, source s makes a commitment $C_i = mc_i\frac{t_i}{N}$ to every forwarding node n_i, and s pays $\frac{c_i}{N}$ for each extra part that n_i forwards beyond t_i. The expected profit of a forwarding node n_i is:

$$\begin{aligned}
\mathrm{E}[\pi_{n_i}] &= [\text{forwarding gains}] - [\text{forwarding \& penalty losses}] \\
&= \left[mc_i\frac{t_i}{N} + \xi_{i_1}\cdot c_i\right] - [\xi_{i_2}\cdot f_i \;+\; \xi_{i_3}\cdot p_{i_a} \;+ \\
&\quad \sigma_i(0|\varphi_{i-1}\geq t_{i-1})[\lambda_{i_a}(\varphi_i\geq t_i)p_{i_a} + \\
&\quad \lambda_{i_b}(\varphi_{i-1}<t_{i-1})p_{i_b}] + \\
&\quad \sigma_{i-1}(0)\lambda_{(i-1)_1}(\varphi_{i-1}\geq t_{i-1})p_{i_b}],
\end{aligned}$$

$$\begin{aligned}
\text{where}\quad \xi_{i_1} &= \frac{m}{N}\sum_{\varphi_i=t_i}^{N}\lambda_{(i+1)_b}(\varphi_i)(\varphi_i - t_i), \\
\xi_{i_2} &= \frac{m}{N}\sum_{\varphi_i=t_i}^{N}\sigma_i(\varphi_i)\varphi_i, \\
\text{and}\quad \xi_{i_3} &= m\left[\sum_{\varphi_i=t_i}^{N}\sigma_i(\varphi_i)\right]\lambda_{(i+1)_b}(0).
\end{aligned}$$

This equation is the difference between what n_i is expected to earn by exceeding threshold t_i when n_{i+1} acknowledges n_i's forwarding actions during forwarding stage in addition to what n_i gains from s's commitment to n_i's bandwidth in the negotiations stage and n_i's expected marginal forwarding costs in addition to expected penalties

when n_i is unable to prove that it meets contractual obligations. Sufficient condition for n_i to forward traffic and make positive profit is for the gains that n_i makes from proper forwarding of s's traffic to be larger than the losses it may incur due to forwarding costs and penalties. Recall that if a node does not meet its threshold, then it is not going to forward anything to avoid extra forwarding costs since in this case it it gets penalized anyway. An important aspect of $\mathrm{E}[\pi_{n_i}]$ is that the profit of n_i depends on the strategies of its neighbors. There is nothing n_i can do if n_{i-1} lies about forwarding at least t_{i-1} parts, and if n_i does not have any confidence in n_{i+1}, then n_i would forward nothing to prevent fruitless forwarding costs. Therefore, a sufficient incentive mechanism must provide n_i with confidence in its neighbors, specifically for n_i to be sure that n_{i+1} acknowledges everything that n_i forwards to n_{i+1}.

The expected profit of the source s is:

$$\begin{aligned}\mathrm{E}[\pi_s] &= [\text{utility}] - [\text{bandwidth costs}] + [\text{penalties}] \\ &= \left[\sigma_\ell(\varphi_\ell \geq t)\sum_{i=1}^{m} u_i\right] - \left[\sum_{i=1}^{\ell}\left[\xi_{i_1} c_i \; + m c_i \frac{t_i}{N}\right]\right] + \\ &\quad m\sum_{i=1}^{\ell}\sigma_i(0|\varphi_{i-1} \geq t_{i-1})(\lambda_{i_a}(\varphi_i \geq t_i)[p_{i_a} + \\ &\quad p_{(i+1)_b}] + \lambda_{i_b}(0|\varphi_{i-1} \geq t_{i-1}) \cdot \\ &\quad [p_{(i-1)_a} + p_{i_b}]).\end{aligned}$$

This equation is the difference between what s is expected to earn from penalties of forwarding nodes in $P_{s\to d}$ when they are unable to prove that they meet contractual obligations in addition to the expected overall utility of batches in b reaching d and what s is expected to pay to all forwarding nodes s has Path-Segment contract with when they exceed their respective thresholds in addition to s's commitment to their bandwidth. If s has high confidence in that $\varphi_\ell \geq t$, then it is sufficient for $\sum_{i=1}^{m} u_i \geq \epsilon_s + \sum_{j=1}^{\ell}(\xi_{j_1} c_j + m c_j \frac{t_j}{N})$ for s to send traffic and make positive profit. If s has no confidence in that $\varphi_\ell \geq t$, and say at least one forwarding node found that it is best for it not to forward; without loss of generality let n_i be the faulty node closest to s (note that there could be multiple faulty nodes on a path, but the closest node drops all the traffic). Then s can still have incentive to send traffic via reimbursement if

$$\frac{1}{m}\left[\sum_{j=1}^{i-2}\xi_{j_1} c_j + \lambda_{i_a}(\varphi_i \geq t_i)\xi_{(i-1)_1} c_{i-1}\right] + \sum_{j=1}^{\ell} c_j \frac{t_j}{N} <$$

$$\lambda_{i_a}(\varphi_i \geq t_i)[p_{i_a} + p_{(i+1)_b}] + \lambda_{i_b}(0)[p_{(i-1)_a} + p_{i_b}].$$

To ensure that s can make positive profit, the CM must enforce penalties to be higher than all of s's expected marginal costs over the whole path $P_{s\to d}$ (see Section 4.2 for further detail), which means that every node's penalty must be at least its forwarding cost. This condition ensures that for no node will it be profitable to advertise bandwidth it does not have, assuming that no forwarding node n_i will agree to a bandwidth cost c_i lower than its forwarding cost f_i. If we assume that s is trusted, then p_{i_a} should be higher than all of s's expected marginal costs. Equation for $\mathrm{E}[\pi_s]$ shows that s might have incentive to send less than N towards d in case $\sigma_\ell(\varphi_\ell > t|\varphi_0 < N)$ is consistently close to 1. This is because, while obtaining only a constant utility u_j for each batch $b_j \in b$ when at least t parts of b_j reach d, s must pay each forwarding node n_i extra for each part of b_j that n_i forwards in excess of t_i parts. However, by the Claiming Shipment Rule (see Section 2.3.1) in this scenario n_1 would not be able to get paid which would cause it drop every batch to prevent fruitless forwarding costs. From penalties, s would not be able to profit at least its minimum settlement ϵ_s due to the structure of penalties as presented in Section 4.2. Therefore, being rational, s would rather send out exactly N parts for each batch.

The following results summarize success of Path-Exchange contracts with respect to definitions of successful mechanism design for contract systems with link-level accountability and proportional payments.

LEMMA 1. *If d is trusted or encouraged with payment $\frac{\epsilon_d}{m}$ to acknowledge receipt of φ_ℓ parts from n_ℓ, this information is known to every participant, and $\sum_{i=1}^{m} u_i \geq \sum_{i=0}^{\ell+1}\epsilon_i + m\sum_{i=1}^{\ell} f_i$, then there is an equilibrium bandwidth price setting $\boldsymbol{c} = \langle c_1, c_2, ..., c_\ell\rangle$ such that at least t parts of every batch in b reach d in the expected case and each element of $P_{s\to d}$ makes a positive profit no less than its respective minimum settlement.*

Lemma 1 satisfies the last part of the definition of successful mechanism design with link-level accountability and proportional payments, and the first two parts of this definition have already been addressed in Section 3.1.

THEOREM 3.1. *Path-Segment contract systems meet definition of successful mechanism design with link-level accountability and proportional payments.*

Theorem 3.1 shows that for Path-Segment contract systems, when every forwarding node is encouraged to forward all traffic as per the contract, at least t parts of each batch in b will reach d in the expected case. However, accountability systems that require to check quality level of each node are inefficient, which is why an accountability system that requires only a constant amount of checking is preferred.

3.2.2 *All-or-Nothing Payments*

The motivation for studying systems with all-or-nothing payments comes from the goal of decreasing the CM's workload by focusing on the overall path efficiency as opposed the efficiency of each node. Overall path efficiency is easier to verify at equilibrium by checking quality of the last link in flow path.

In this scenario, everything is the same as in the scenario with link-level accountability described in the previous subsection with the exception that punishment is administered only when the amount of parts n_ℓ forwards φ_ℓ is less that overall path threshold t and payment is not proportional to the amount of parts forwarded. We will perform the same analysis as for the scenario with proportional payments.

When an agreement is reached in the negotiations stage, s commits $mc_i \frac{t_i}{N}$ to every forwarding node n_i. As long as $\varphi_\ell \geq t$, every node n_i gets paid a fixed bandwidth cost $c_i \frac{t_i}{N}$, otherwise each node n_i has to prove that it met its threshold t_i in order to get paid. Note the use of Assumption 2 (independence) for profit analysis. The expected profit of forwarding node n_i is :

$$\begin{aligned}
\mathrm{E}[\pi_{n_i}] &= [\text{gains from forwarding}] - [\text{losses from penalties}] \\
&= \left[mc_i \frac{t_i}{N}\right] - [\xi_{i_1} + \xi_{i_2} + \\
&\quad m\sigma_i(0|\varphi_{i-1} \geq t_{i-1})[\lambda_{i_a}(\varphi_i \geq t_i) \cdot \\
&\quad p_{i_a} + \lambda_{i_b}(\varphi_{i-1} < t_{i-1})p_{i_b}] + \\
&\quad m\sigma_{i-1}(\varphi_{i-1} < t_{i-1})\lambda_{(i-1)_1}(\varphi_{i-1} \geq t_{i-1})p_{i_b}],
\end{aligned}$$

$$\begin{aligned}
\text{where} \quad \xi_{i_1} &= m \sum_{\varphi_i = t_i}^{N} \sigma_i(\varphi_i) \left(\frac{\varphi_i}{N} f_i + \lambda_{(i+1)_b}(\varphi_i < t_i) p_{i_a}\right) \cdot \\
&\quad (1 - \sum_{\varphi_{i+1}=t}^{\varphi_i} \binom{\varphi_i}{\varphi_{i+1}} \sigma_{i+1}(\varphi_{i+1}) [\cdots] \\
&\quad \left[\cdots \left[\sum_{\varphi_\ell = t}^{\varphi_{\ell-1}} \binom{\varphi_{\ell-1}}{\varphi_\ell} \sigma_\ell(\varphi_\ell)\right] \cdots\right]),
\end{aligned}$$

$$\begin{aligned}
\text{and} \quad \xi_{i_2} &= m \sum_{\varphi_i = t}^{t_i - 1} \sigma_i(\varphi_i)(\lambda_{i_a}(\varphi_i \geq t_i) p_{i_a} + \\
&\quad \lambda_{i_b}(\varphi_{i-1} < t_{i-1}) p_{i_b} + \frac{\varphi_i}{N} f_i) \cdot \\
&\quad (1 - \sum_{\varphi_{i+1}=t}^{\varphi_i} \binom{\varphi_i}{\varphi_{i+1}} \sigma_{i+1}(\varphi_{i+1}) [\cdots] \\
&\quad \left[\cdots \left[\sum_{\varphi_\ell = t}^{\varphi_{\ell-1}} \binom{\varphi_{\ell-1}}{\varphi_\ell} \sigma_\ell(\varphi_\ell)\right] \cdots\right]).
\end{aligned}$$

This equation is very similar to the one for proportional payments; the differences are that a node's gain is fixed to the commitment and that node's losses due to penalties depend on whether the final node n_ℓ meets its threshold t. Just as in the scenario with proportional payments, sufficient condition for n_i to forward traffic and make positive profit is for the gains that n_i makes from forwarding to be larger than the losses it may incur due to penalties. Besides n_i's confidence in its neighbors, n_i's confidence in whether $\sigma_\ell(\varphi_\ell > t)$ is high is important. If $\sigma_\ell(\varphi_\ell > t)$ is high, n_i may be encouraged to forward $t \leq \varphi_i \leq t_i$ in order to prevent extra losses due to forwarding. Therefore, sufficient incentive mechanism must provide n_i with confidence in its neighbors and make it unprofitable to economize on forwarding costs.

Expected profit equation of s is:

$$\begin{aligned}
\mathrm{E}[\pi_s] &= [\text{utility}] - [\text{commitments}] + [\text{penalties}] \\
&= \left[\sigma_\ell(\varphi_\ell \geq t) \sum_{i=1}^{m} u_i\right] - \left[\sum_{i=1}^{\ell} \xi_{i_1} c_i\right] + \\
&\quad \sigma_\ell(\varphi_\ell < t)\, m \sum_{i=1}^{\ell} \sigma_i(\varphi_i < t_i | \varphi_{i-1} \geq t_{i-1}) \cdot \\
&\quad (\lambda_{i_a}(\varphi_i \geq t_i)[p_{i_a} + p_{(i+1)_b}] + \lambda_{i_b}(\varphi_{i-1} < t_{i-1}) \cdot \\
&\quad [p_{(i-1)_a} + p_{i_b}]).
\end{aligned}$$

The main difference between this equation and that of source's profit in the proportional payments case is that in the case of all-or-nothing payments the source does not have to pay to forwarding nodes more than the commitment and failure is addressed only if n_ℓ does not meet t. If s has high confidence in that $\varphi_\ell \geq t$, then it is sufficient for $\sum_{i=1}^{m} u_i \geq \epsilon_s + \sum_{j=1}^{\ell} mc_j \frac{t_j}{N}$ for s to send traffic and make positive profit. If s has no confidence in that $\varphi_\ell \geq t$, and say at least one forwarding node found that it is best for it not to forward anything at all; without loss of generality let the closest faulty node to s be n_i. Then s can still have incentive to send traffic via reimbursement if

$$\sum_{j=1}^{\ell} c_j \frac{t_i}{N} <$$

$$\lambda_{i_a}(\varphi_i \geq t_i)[p_{i_a} + p_{(i+1)_b}] + \lambda_{i_b}(\varphi_{i-1} < t_{i-1})[p_{(i-1)_a} + p_{i_b}].$$

Just as in the scenario with proportional payments, to ensure that s can makes positive profit, the CM must enforce penalties to be higher than all of s's expected marginal costs over the whole path $P_{s \to d}$.

LEMMA 2. *If d is trusted or encouraged with payment $\frac{\epsilon_d}{m}$ to acknowledge receipt of φ_ℓ parts from n_ℓ, $p_{i_a} < p_{i_b}\ \forall\ 1 \leq i \leq \ell$, this information is known to every participant, and $\sum_{i=1}^{m} u_i \geq \sum_{i=0}^{\ell+1} \epsilon_i + m \sum_{i=1}^{\ell} f_i$, then there are equilibrium bandwidth price and penalty settings $\boldsymbol{c} = \langle c_1, c_2, ..., c_\ell \rangle$ and $\boldsymbol{p}_1 = \langle p_{1_1}, p_{2_1}, ..., p_{\ell_1} \rangle$, respectively, such that exactly t parts of every batch in b reach d, each element of $P_{s \to d}$ makes a positive profit no less than its corresponding minimum settlement, and the CM only has to check a single proof of receipt, namely, proof that $\varphi_\ell = t$ provided by d, per round.*

Lemma 1 satisfies the last part of the definition of successful mechanism design with link-level accountability and all-or-nothing payments, and the first two parts of this definition have already been addressed.

THEOREM 3.2. *Path-Segment contract systems meet definition of successful mechanism design with link-level accountability and all-or-nothing payments.*

3.3 Failure of Pairwise-Exchange Contracts

In Pairwise-Exchange contract systems source's utility is defined the same way as in the Path-Segment contract systems, but we also need to introduce the utility u_{n_i} of each

forwarding node $n_i \in P_{s\to d}$ which n_i gains when its receiver on path $P_{s\to d}$ (i. e. n_{i+1}) meets contractual obligations. For our analysis we are going to assume that u_{n_i} is defined as the payment $c_i\frac{t_i}{N}$ which n_i receives from n_{i-1} when the former can prove to the latter that n_i forwarded a batch in b correctly. We also assume that u_{n_i} is the same for each batch in b for all forwarding nodes in the game except for the source s. $u_{n_0} = 0$ because source s does not gain anything when n_1 forwards a batch $b_j \in b$ of s to n_2 (unless $\ell = 1$ in which case u_{n_0} is defined according to $u_{1\le j\le m}$), unless at least t packets of b_j make it to d, in which case s gains u_j. We see that $\sum_{j=1}^{m} u_j > mc_1+\epsilon_s$ and $c_i-f_i \ge c_{i+1}+\epsilon_{n_i}\ \forall\, 1 \le i \le \ell-1$ are necessary conditions for s's traffic to reach d. Below, we analyze two scenarios where Pairwise-Exchange contract systems fail due to problems that stem from these necessary conditions. The first problem arises due to inaccuracies of estimation of traffic patterns on the Internet and how such inaccuracies propagate given the second necessary condition above, while the second problem arises due to inability of AD requesting connectivity to negotiate traffic service level separately for each destination. By contractual failure we refer to the scenario where s has enough funds to pay each node along an available (bandwidth up for sale) flow path to d at least that node's minimum settlement in addition to the forwarding cost, but s is unable to reach d due to depeering along that path, which is defined as follows.

DEFINITION **Depeering** *Depeering* of adjacent nodes A and B is an agreement made during the negotiations stage to not exchange any traffic during the forwarding stage. ■

We conclude this section with a presentation of necessary and sufficient requirements for Pairwise-Exchange contracts to avoid contractual failures and satisfy both link-level success definitions. Proofs of Lemma 3 and Theorems 3.3 and 3.4 are sketched in our technical report [29].

3.3.1 *Depeering Due to Traffic Estimation Error*

Accurate estimation of traffic patterns on the Internet is difficult task, and in this subsection we show how errors made during traffic estimation can result in contractual failures. Consider a scenario depicted in Figure 1. Bandwidth costs $c_{1\le i\le \ell}$ are per batch of size N. For this example we assume that s is the only traffic generator. Considering the necessary conditions for traffic to flow in Pairwise-Exchange contract systems mentioned above it must be the case that $c_i - f_i \ge \sum_{j=i+1}^{\ell} c_j + \epsilon_{n_i}\ \forall\ 1 \le i \le \ell$ to account for all marginal costs of n_i. Thus, when s is the only generator of traffic and s wants to send a batch to d, s must spend at least $f_1 + \sum_{j=2}^{\ell} c_j + \epsilon_{n_1}$ whether $P_{s\to d}$ was formed via Pairwise-Exchange or Path-Segment contracts, where f_1 is n_1's marginal cost for forwarding a batch of size N. Now, let us say that s changes its destination of interest to some $n_{1<i<\ell}$. When $P_{s\to d}$ is formed via Pairwise-Exchange contracts, for delivering a batch to the new destination s could be required to pay n_1 no less than $f_1 + \sum_{j=2}^{i-1} c_j + \epsilon_{n_1}$ and $f_1 + \sum_{j=2}^{\ell} c_j + \epsilon_{n_1}$ if n_{i-1} does and does not account for the fact that n_{i-1} does not need to pay n_i to route s's traffic in this situation respectively. Such a correction is subject to contract negotiation between n_{i-2} and n_{i-1} and is feasible in our model.

In a more complex situation, say s wants to deliver approximately $Y\%$ of its traffic to n_i and the rest to d over a period of time long enough for n_{i-1} to notice this distribution. This distribution may change from game to game (negotiations and forwarding stages repeated many times). Even though s cannot specify its flow distribution, n_{i-1} can try to estimate it over time with some error $\pm\delta$ representing maximal deviation and charge n_{i-2} for expected $Y \pm \delta\%$ of traffic that needs to go through n_{i+1}. More realistically, since n_{i-1} is selfish, it is in its best interest to always overestimate the amount of traffic that flows through n_i and charge n_{i-2} for $Y + \delta\%$ of traffic, which is the maximal amount of traffic s may send to d. In real world scenario with many different flows, n_{i-1} could allocate $Y+\delta\%$ worth of bandwidth to prevent congestion in case volume of traffic from s to d does reach $Y + \delta\%$. Assuming that every forwarding node's penalty for not meeting contractual obligations is high enough to prevent lying about resources during the negotiations stage (see Section 3.1 for detail), this overestimation will propagate to s as required by the necessary conditions mentioned above. Although it is in the best interest of every $n_{1\le j\le i-1}$ to overestimate, for simplicity we will assume that only n_{i-1} overestimates in this example (the final result without this simplification is analagous). Therefore, s will be required to pay n_1 at least $f_1 + \frac{\epsilon_{n_1}}{m} + (\frac{1}{2} - \delta)\sum_{j=2}^{i-1} c_j + (\frac{1}{2} + \delta)\sum_{j=1}^{\ell} c_j$ per batch which is greater than $f_1 + \frac{\epsilon_{n_1}}{m} + \frac{1}{2}\sum_{j=1}^{i-1} c_j + \frac{1}{2}\sum_{j=1}^{\ell} c_j$ when $\delta > 0$. We see that if at negotiations stage of some repetition of the game s's overall utility for having exactly $Y\%$ of its traffic delivered to n_i and the rest to d is $mf_1 + \epsilon_{n_1} + m\frac{1}{2}\sum_{j=1}^{i-1} c_j + m\frac{1}{2}\sum_{j=1}^{\ell} c_j + \epsilon_s$, then s and n_1 will depeer. This result can be easility extended to the case where every node overestimates traffic more expensive traffic and underestimates cheaper traffic.

The problem of estimation error propagation is not an issue in path-based contract systems because in such systems s can negotiate each flow with each forwarding node separately.

3.3.2 *Depeering Due to Flow Inseparability*

In Pairwise-Exchange contracts, unlike in Path-Segment contracts, negotiations are coarse grained; AD requesting connectivity cannot negotiate traffic service level for each destination separately because traffic to all destinations is treated equal under Pairwise-Exchange Contracts. In this section we show how such coarse granularity may result in contractual failure. Consider the scenario depicted in Figure 2. In this situation node X is a service provider for n sources $s_1, s_2, \ldots, s_n$. Every source wants to send 1 unit of traffic to the next hop of each of D_1 and D_2 which are service providers for X. D_1 is also a service provider of s_0. Utilities of the sources are as follows:

- $u_{s_1\to D_1} = c_1+c_x+\epsilon_{s_1}^{D_1}$ and $u_{s_1\to D_2} = \frac{c_2}{n}+c_x+\epsilon_{s_1}^{D_2}$,

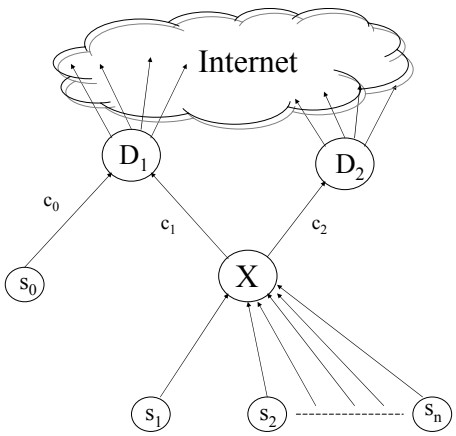

Figure 2: Setup where depeering may occur due to inseparability of flows between adjacent nodes during negotiations stage.

where $\epsilon_{s_1}^{D_1} > \epsilon_{s_1}^{D_2}$;

- $u_{s_i \to D_1} \approx 0$ and $u_{s_i \to D_2} = \frac{c_2}{n} + c_x + \epsilon_{s_i}^{D_2} \ \forall\, 1 < i \leq n$.

Here $\epsilon_{s_i}^{D_j}$ is the minimum profit s_i can settle for when buying connectivity to D_j. The negotiations in this example start with s_0. None of the players knows u_{s_0}, but s_0 offers D_1 to purchase all of its bandwidth at a bandwidth cost of $\frac{c_0}{n}$ per unit. With such leverage, D_1 offers X n units of bandwidth at a price of $c_1 = \frac{c_0}{n} + \delta'$ per unit for some $\delta' > 0$. D_2 offers X n units of bandwidth at a price of $\frac{c_2}{n}$ per unit. To its clients, X advertises access to D_1 and D_2, and through negotiation X figures out what each s_i is willing to pay. These a advertisements are subject to contract negotiations between X and $s_{1 \leq i \leq n}$ and are feasible in our model. Considering that X charges c_x per unit of bandwidth to cover forwarding costs and make positive profit respecting X's minimum settlement, the most X could make is:

$$(n-1)(\frac{c_2}{n} + c_x) + c_1 + c_x - nc_1 - c_2 =$$

$$c_2 + nc_x - \frac{c_2}{n} - c_x + c_1 + c_x - nc_1 - c_2 =$$

$$nc_x - \frac{c_2}{n} - (n-1)c_1.$$

However, were X to advertise access to only D_2, X's maximum profit could be:

$$n(\frac{c_2}{n} + c_x) - c_2 = c_2 + nc_x - c_2 = nc_x.$$

Assuming that X's penalty for not meeting contractual obligations is high enough to prevent X from lying about its resources during the negotiations stage (see Section 3.1 for detail), when $n \geq 1$ it is rational for X and D_1 to depeer. This is unfortunate for s_1 considering the facts that s_1 would rather send 1 unit of traffic to a destination one hop after D_1 than to a destination one hope after D_2 and s_1's utility allows s_1 to pay X and D_1 for a path going through them. Such problem could not be an issue in path-based contract systems because in such systems s can negotiate each flow with each forwarding node separately.

3.3.3 *Modifications to Pairwise-Exchange Contracts*

While Path-Segment contract systems provide the source with more options over the quality of the path than Pairwise-Exchange contract systems do, the former result in much higher penalties for long paths and require more resources to set up and at equilibrium. In this subsection we show that the extra resources required to set up Path-Segment contract systems may be necessary in order to provide better guarantees to the source of traffic. Examples mentioned above show that Pairwise-Exchange contract systems satisfy neither one of the definitions of successful mechanism design for contract systems with accountability because in situations where s may have enough resources to pay for a path $P_{s \to d}$ it might not be always able to purchase this connectivity due to depeering. We see how these examples would never happen in Path-Segment contract systems where s can negotiate each flow separately.

LEMMA 3. *Requiring entities to negotiate Pairwise-Exchange contracts with per-flow granularity is a necessary and sufficient condition to prevent contractual failures in Pairwise-Exchange contract systems.*

THEOREM 3.3. *Contract systems based on Pairwise-Exchange contracts that require negotiation at per-flow granularity meet definition of successful mechanism design with link-level accountability and proportional payments.*

Even if the requirement to negotiate Pairwise-Exchange contracts per flow is adopted, meeting success definition for contract systems with link-level accountability and all-or-nothing contract systems is not possible for Pairwise-Exchange contract systems because no participant including the CM in such systems accounts for the overall quality of a path $P_{s \to d}$, only quality of adjacent neighbors is monitored.

THEOREM 3.4. *Requiring the CM to monitor the quality of overall flow paths is a necessary and sufficient condition for contract systems based on Pairwise-Exchange contracts that require negotiation at per-flow granularity to meet definition of successful mechanism design with link-level accountability and all-or-nothing payments.*

Theorems 3.3 and 3.4 show that with some modifications Pairwise-Exchange contract systems may achieve comparable level of guarantee as Path-Segment contract systems at the expense of extra resources. Nevertheless, Pairwise-Exchange intrinsically cannot provide the level of choice of service level to the source that Path-Segment contracts do.

4. Attacks and Defenses

This section discusses possible issues when nodes collude to gain and/or behave maliciously in order to gain profit in the short or long run. We start by describing attacks that stem from the fact that it may be profitable for participants to lie about their resources and behavior, and we suggest possible remedies by specifying what the bandwidth commitments and penalties should be for Path-Segment and

Pairwise-Exchange contract systems respecting the success definitions presented in Section 2.4. We finish on a negative note by showing why depeering cannot be prevented in the face of participants whose utility to do malice is unknown.

4.1 False Advertisements

We describe an attack that Pairwise-Exchange contract systems may be vulnerable to, unlike Path-Segment contract systems, and motivate the need for mechanisms to construct penalties that could prevent this attack.

For some path $P_{s\to d}$, bandwidth costs increase at some node, and this increase begins to propagate in the direction of the source. Let us assume that $P_{s\to d}$ is the only path from s to d. Let us look at the strategy space of some node n_i on the path of the propagation of the bandwidth cost increase:

1. increase its bandwidth cost c_i, thereby contributing to the propagation;
2. depeer from n_{i+1} if n_i expects to lose money from this peering;
3. decrease the amount of traffic that passes through n_i along $P_{s\to d}$ by dropping any excess.

Strategy 3 yields an attack where some intermediary node drops s's traffic without s even being warned because s never notices the price increase. To prevent this attack it is enough for the CM to ensure during the negotiations stage that penalties for each node are higher than that node's forwarding cost (see 4.2 for ways to ensure this). Neither of the strategies (1-3) of n_i makes sense in Path-Segment contract systems because c_i is not directly related to c_{i+1}, since n_i does not have a direct contract with n_{i+1}, in Path-Segment contract systems the source will never be left blind with respect to bandwidth cost increases. The latter holds because the source is required to purchase the whole path $P_{s\to d}$ thereby inevitably finding out the bandwidth cost of each link on $P_{s\to d}$. Therefore, this scenario does not happen in Path-Segment contract systems.

4.2 The Right Commitments and Penalties

In this subsection we discuss two attacks in order to motivate mechanisms for specifying bandwidth commitments and penalties which we present at the end of this subsection.

Our analysis of contract systems assumes that s is trusted. However, in link-level accountability settings, were we to relax this assumption, in cases where s can make more money by lying about sending traffic and collecting penalties from n_1 than from sending messages to the destination d, s would rather lie. To address this issue the CM must make sure that s's utility for every batch that reaches d is higher than what s could gain form penalties of nodes it has contracts with. However, this is very challenging to achieve if s's valuation of each successful delivery is different, so we are going to assume that $u_i = u_{j\neq i}\ \forall\ 1 \leq i \leq m$.

With link-level accountability, a source s may gain profit by colluding with a forwarding node n_i if blaming a neighbor of n_i could yield a positive profit in penalties that s and n_i could split. Let us assume that $\frac{C_j}{m} < c_j$ for $j = i-1$ or $j = i+1$ (depending on whom s colludes with). In Pairwise-Exchange contract systems, this collusion attack can be done only in groups of three adjacent nodes. The left-most node in the group colludes with one other node in the group against the third one in the group. For Path-Segment contract systems with link-level accountability the two nodes that share the faulty link must pay for themselves and the rest of the path to compensate for s's expenses. Without loss of generality let us say that s colludes with n_i to drop packets and blame n_{i+1}. Then, in a fair-penalty case, the CM must collect n_i's and n_{i+1}'s penalties of more than $c_i + \frac{1}{2}\sum_{k=1}^{i-1} c_k + \frac{1}{2}\sum_{k=i+2}^{\ell}\frac{C_k}{m}$ and more than $c_{i+1} + \frac{1}{2}\sum_{k=1}^{i-1} c_k + \frac{1}{2}\sum_{k=i+2}^{\ell}\frac{C_k}{m}$ respectively. Thus, to prevent collusion the CM could simply make sure that $c_i \leq \frac{1}{2}\sum_{k=1}^{i-1} c_k + \frac{1}{2}\sum_{k=i+2}^{\ell}\frac{C_k}{m}$ and $c_i \leq \frac{1}{2}\sum_{k=1}^{i-2} c_k + \frac{1}{2}\sum_{k=i+1}^{\ell}\frac{C_k}{m}, \forall\ 1 \leq i \leq \ell$. However this condition is impossible to meet when $\ell < 4$ for Path-Segment contract systems, which implies that it is impossible to meet for Pairwise-Exchange contract systems in general.

To prevent collusion, the CM must ensure that every entity's commitments and every forwarding node's penalties render collusion and dropping traffic in general unprofitable. To defend against these attacks we, first, propose that a commitment must be equal to the total cost of bandwidth, $C_i = mc_i\ \forall\ 1 \leq i \leq \ell$, for both Path-Segment and Pairwise-Exchange contract systems. This prevents the attack described in the paragraph above. Also, for Path-Segment contract systems, n_i's penalty must be at least $\frac{C_i}{m} = c_i$ in addition to some fraction $\eta_i < 1$ of s's minimum settlement $\frac{\epsilon_s}{m}$ per batch and some fraction of the path excluding itself and the other node sharing the faulty link. For settings with link-level accountability, this ensures that both nodes sharing the faulty link, say n_i and n_{i+1}, pay for the whole path in addition to a fraction $\frac{\eta_i+\eta_{i+1}}{m} < \frac{1}{m}$ of s's minimum settlement $\frac{\epsilon_s}{m}$ per batch. For Pairwise-Exchange contract systems, we require that every node n_i who can claim shipment (see Claiming Shipment Rule, Section 2.3.1) obtains payment equal to commitment $\frac{C_{i+1}}{m}$ in addition to a fraction $\eta_i < 1$ of $\frac{\epsilon_{n_i}}{m}$ per batch from n_{i+1} if n_{i+1} shares the faulty link. From n_i's point of view, the values of p_{i_a} and p_{i_b} are $\left[\frac{C_{i+1}}{m} + \eta_i\epsilon_{n_i}\right] - \left[\frac{C_i}{m} + \eta_{i-1}\epsilon_{n_{i-1}}\right]$ and $\frac{C_i}{m} + \eta_{i-1}\epsilon_{n_{i-1}}$ respectively, so to make it unfavorable for nodes to drop traffic and to prevent the attack presented in Section 4.1 it is sufficient for $\epsilon_{n_i} > \eta_i\epsilon_{n_i} - \eta_{i-1}\epsilon_{n_{i-1}}$ to hold. This condition is trivially satisfied as long as CM makes sure that $0 < \eta_i < 1\ \forall\ 1 \leq i \leq \ell$. For both Path-Segment and Pairwise-Exchange contract systems it is important that the overall profit an entity may gain from penalties is less than that entity's minimum settlement, otherwise an entity could simply not send anything and make at least its minimum settlement from collected penalties by blaming the next node down stream. Enforcing this condition for each entity during the negotiations stage while not knowing that entity's minimum settlement directly is a challenge that we have not yet encountered a solution to.

4.3 Malicious Intent

Although we have presented sufficient conditions for functional contract systems where nodes are discouraged from being faulty, our model does not address two important issues for settings with link-level accountability: out of malice (i) forwarding nodes may selectively drop traffic of non-adjacent competitors and blame neighbors for poor quality, and (ii) forwarding nodes may have incentive for destroying adjacent competitors' reputation by dropping traffic and blaming that adjacent node for poor quality. Both cases may result in depeering. In Pairwise-Exchange contract systems depeering is achieved by at least one neighbor refusing to establish a Pairwise-Exchange contract with the malicious party, and in Path-Segment contract systems depeering is achieved by an entity refusing to advertise the link that connects it to the malicious party. Some participants may have incentive for doing (i), (ii), or both regardless of what the penalties are if such actions may be of profit in the long run or simply out of malicious intent. **The biggest disadvantage of Pairwise-Exchange systems is that in the face of attacks motivated by irrational malicious intent s never gets reimbursed.** The CM cannot provide incentive for malicious parties to meet contractual obligations because it has no way of figuring out how to penalize them. While there seems to be no solution for case (ii), case (i) can be addressed as follows. Each forwarding node could verifiably encrypt (e.g. [7]) each packet prior to forwarding it to the next node on the path and require proof of receipt before revealing the decryption key. Overall, this procedure works only as long as for every node there is a traffic flow which would result in an overall loss were that node to drop it, so penalties should heavily depend on the source of the traffic. The latter property is intrinsic to Path-Segment contract systems because in such systems negotiations are performed at per-flow granularity and penalties are high enough to pay for the whole flow path in addition to a fraction of the source's minimum settlement. This, however, does not hold for Pairwise-Exchange contracts because, as we saw in Section 3.3, negotiations do not distinguish quality of service at flow granularity. Modification that allows Pairwise-Exchange contracts be negotiable at per-flow granularity, as discussed in Section 3.3.3 provides parties involved in Pairwise-Exchange contract systems with a way to resolve issue (i).

5. Related Work

There has been much work related to accountability and incentive mechanism design on the Internet. We discuss recent research in the areas of network accountability and fault localization, followed by a review of related work in price and incentive mechanism design for wireless as well as wireline networks.

5.0.0.1 Accountability and Fault Localization.

In [23] and [8], use of encryption and multi-path routing was proposed to guarantee delivery of packets and preventing failures. Were these proposals not too impractical with respect to computation and bandwidth overhead, accountability and contract policing would not be an important issues.

A secure quality monitoring and link-level fault localization mechanism proposed by Avramopoulos and Rexford, called stealth probing [4], uses a combination of active probing via IPsec technology and byzantine tomography (network tomography used to identify faulty links with probing). Unfortunately, stealth probing is impractical as it requires encryption of all traffic. Secure Traceroute, a link-level accountability scheme, based on marking packets as probes via secret identifiers, is presented in [22]. Argyraki et al. present in [3] another link-level accountability scheme AudIt, where each AD sends feedback per flow to traffic sources regarding loss and delay. As pointed out in [5], the major problem with these two approaches is that an adversary could frame any AD by dropping that AD's feedback. Barak et al. propose yet another link-level accountability scheme that is secure even in the presence of adversaries [5]. This scheme relies on the assumptions that there is only a single adversary, communication channels are single bi-directional paths, and that sources and destinations trust each other. This accountability scheme has a similar weakness as Secure Traceroute and AudIt with respect to multiple indenpendent adversaries (see our technical report for further treatment [29]). The reader should note that all three accountability schemes [3, 5, 22] suffer from the absence of trusted channels between entities, something we believe to be necessary for successful accountability systems in presence of multiple independent adversaries. For our work we assume that every participant must have a trusted channel with the trusted authority, the CM, in order to avoid this issue.

5.0.0.2 Price and Mechanism Design.

In [20] the use of Vickrey-Clark-Groves (VCG) mechanism was shown by Nisan and Ronen to accurately solve the shortest-path problem with selfish nodes, and later mechanisms based on VCG have been proposed for lowest-cost routing in wireline and wireless networks in [11] and [2], respectively. While the mechanism discussed in [11] is mostly based on BGP where all pairs of nodes want to communicate, the mechanism developed in [2] is appropriate for ad hoc networks where not all pairs of nodes may want to communicate and is more targeted towards forming complete paths. In SPRITE [28], the authors present a payment mechanism for wireless setting where every node is discouraged from being dishonest. MINT, a market design based on continuous double auction administered by a mediator along with a suite of routing protocols is proposed in [26].

Valancius et al. show that in MINT, ISP's and edge networks can make bids regarding desired connectivity as buyers, and they can make advertisements regarding available bandwidth as sellers to a central authority. The latter is responsible for matching demand of buyers with suitable supply of sellers such that buyers end up purchasing a single path with satisfactory characteristics. Assuming support of a central trusted authority in MINT makes its market framework very helpful in establishing contract systems, and, as detailed in Section 2, we use this assumption in our models. Neither of these mechanisms has yet been analyzed by the research community with respect to different accountability settings. In [9] it was shown by Elkind et al. that any truth-

ful mechanism for purchasing a shortest path may require the buyer to pay possibly more than twice the cost of that shortest path. However, we do not consider the problem of truthfulness in price negotiations to be related to our study as long as participants do not advertise resources they do not possess. This is because our objective is to ensure that nodes are not faulty with respect to traffic, regardless of whether these nodes advertise their true bandwidth costs honestly.

The most related study to our work is by Laskowski and Chuang where the authors show that without a proper accountability framework innovation and optimal routes on the Internet are impossible [16]. Laskowski and Chuang propose a general node-level accountability framework that employs trusted entities that monitor the quality and optimality of each path in order to enforce accountability and ensure path optimality at equilibrium for pairwise contract systems. Presence of such monitors renders the problem of fault localization trivial, but the implementation of such monitors in real life is impractical. Also, the node-level accountability scheme proposed in [16] does not focus on fault-localization per se, and it is proven to work only under the assumption that there can be only one adversary (or a single contiguous collusion of adversaries) on a path, a weakness we address in our technical report [29]. We do not focus on node-level accountability due to its impracticality and instead assume existence of a link-level accountability scheme secure against multiple independent adversaries. Also, instead of concentrating on path optimality we address the issue of entities meeting a promised level of service when forwarding traffic along a

6. Conclusion and Future Work

In order for network administrative domains to have incentives to fulfill their promises to their business partners, in this work we have, first, motivated the need for network administrative domains to formalize business agreements into concrete contracts and, second, to use accountability frameworks in order to make contracts enforceable. We review our contributions. We formally define path-based contracts and pairwise contracts, and we present sufficient conditions for path-based contract systems and accountability frameworks that guarantee networks along a path have an incentive to meet their respective contractual obligations. We show that pairwise contract systems may suffer from depeering in situations with available bandwidth and sufficient demand, failures path-based contracts are safe from, and propose sufficient modifications for preventing such failures in pairwise contract systems and show that pairwise contract systems may meet the same level of guarantee as path-based contract systems at extra computational cost. We present conditions for path-based and pairwise contract systems sufficient to allow only a constant amount of monitoring for every participant to make a positive profit at an equilibrium where participants are discouraged from being faulty. We present examples of attacks of selfish but rational entities for path-based and pairwise contract systems and propose solutions to these attacks. Lastly, we discuss possibly unpreventable issue of malicious parties causing depeering in pairwise and path-based contract systems, and we show that path-based contracts allow the sender of traffic to get reimbursed which cannot be guaranteed for pairwise contract systems.

For future work we leave the following problems: designing an incentive mechanism and analyzing contract systems that are not limited to a single path; designing a negotiation scheme that minimizes the number of negotiation rounds before either a contract can be established or an incompatibility is found; presenting minimal requirements for a node-level accountability and/or link-level accountability schemes assuming multiple independent adversaries.

REFERENCES

[1] M. Afergan and J. Wroclawski, "On the Benefits and Feasibility of Incentive Based Routing Infrastructure," In *PINS*, 2004.

[2] L. Anderegg, S. Eidenbenz, "Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents," Proc. *ACM MobiCom*, pp. 245259. 2003.

[3] K. Argyraki, P. Maniatis, O. Irzak, S. Ashish, S. Shenker, "Loss and Delay Accountability for the Internet," Proc. *IEEE International Conference on Network Protocols ICNP*, 2007.

[4] I. Avramopoulos and J. Rexford, "Stealth probing: Data-plane security for IP routing," Proc. *USENIX*, 2006.

[5] B. Barak, S. Goldberg, and D. Xiao, "Protocols and Lower Bounds for Failure Localization in the Internet," Proc. *EUROCRYPT*, 2008.

[6] S. Buchegger, J. Le Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," Proc. *IEEE Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing*, pp. 403 - 410, 2002.

[7] J. Camenisch and V. Shoup, "Practical Verifiable Encryption and Decryption of Discrete Logarithms," Proc. *CRYPTO 2003*, 2003.

[8] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly Secure Message Transmission," Journal of the *ACM*, 40(1), 1993.

[9] E. Elkind, A. Sahai, K. Steiglitz, "Frugality in Path Auctions," *ACM-SIAM* Symposium on Discrete Algorithms (*SODA*), 2004.

[10] C. Estan and A. Akella and S. Banerjee, "Achieving Good End-to-End Service Using Bill-Pay," *HotNets*, 2006.

[11] J. Feigenbaum, Ch. Papadimitriou, R. Sami, S. Shenker,"A BGP-based Mechanism for Lowest-Cost Routing," Proc. *21st ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 173-182, 2002.

[12] S. Goldberg, D. Xiao, B. Barak, J. Rexford, and E. Tromer, "Path-Quality Monitoring in the Presence of Adversaries," Proc. *ACM SIGMETRICS*, 2008.

[13] V. Jacobson, "Congestion Avoidance and Control," Proc. *ACM SIGCOMM '88*, pp. 314-329, 1988.

[14] F. P. Kelly, "Charging and rate control for elastic traffic," *European Transactions on Telecommunications*, vol. 8, pp. 3337, 1997.

[15] F. P. Kelly, A. K. Maulloo, and D. K. Tan, "Rate control for communication networks: shadow prices, proportional fairness, and stability," *Journal of the Operational Research Society*, vol. 49, pp. 237252, 1998.

[16] P. Laskowski, J. Chuang, "Network Monitors and Contracting Systems: Competition and Innovation," Proc. *SIGCOMM*, 2006.

[17] J. K. MacKie-Mason and H. R. Varian, "Pricing the Internet," In B. Kahin and J. Keller, editors, *Public Access to the Internet*, pages 269314. *MIT Press*, Cambridge, Massachusetts, 1995.

[18] S. Marti, T. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proc. *Sixth International Conference on Mobile Computing and Networking*, 2000.

[19] P. Michiardi, R. Molva, "CORE: A Collaborative Repudiation Mechanism to enforce node cooperation in Mobile Ad hoc Networks," Proc. *CMS 2002*, 2002.

[20] N. Nisan, A. Ronen, "Algorithmic Mechanism Design," Proc. *STOC 1999*.

[21] A. M. Odlyzko, "Paris Metro Pricing for the Internet," Proc. *ACM Conference on Electronic Commerce (EC)*, pp. 140147, 1999.

[22] V. N. Padmanabhan and D. R. Simon, "Secure Traceroute to Detect Faulty or Malicious Routing," Proc. *SIGCOMM*, 2003.

[23] R. Perlman, "Network Layer Protocols with Byzantine Robustness," PhD thesis, MIT, 1988.

[24] A. Popescu and T. Underwood, "D(3) Peered: Just the Facts Ma'am, A Technical Review of Level (3)s Depeering of Cogent," *NANOG 35*, 2005.

[25] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, "Hash-Based IP Traceback," Proc. *SIGCOMM*, 2001.

[26] V. Valancius, N. Feamster, R. Johari, V. Vazirani, "MINT: A Market for INtenet Transit," ReArch'08 - Re-Architecting the Internet, 2008.

[27] W. Xu and J. Rexford, "MIRO: Multi-path Interdomain ROuting," Proc. *SIGCOMM*, 2006.

[28] S. Zhong, Y. R. Yang, J. Chen, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-hoc Networks," Proc. *INFOCOM 2003*, pp. 1987-1997, 2003.

[29] Technical report, removed for anonymity. Contact *SIGCOMM* PC chairs to obtain a copy.

Appendix

A. Sketch of a Proof of Shipment Protocol and Vulnerabilities of Some Accountability Schemes

A.1 Proofs of Shipment

Let us define procedure $ProofOfShipment(x, m, y)$ as a procedure that consists of an entity x sending a message m to y distinct neighbors followed by receiving and recording the proof of receipt of this message by at least one neighbor. $ProofOfShipment()$ can be used by any participant of the network to obtain a proof of shipment of a message by acquiring a proof of receipt of that message from at least one of its neighbors. In practice a secure summarization procedure, such as the one presented in [12], could be used to generate proofs of receipt. This idea is similar to what has been proposed in [23] and [8] in order to guarantee delivery of packets at the cost of very high computation and bandwidth overhead. The main weakness of this approach are it is wasteful in terms of bandwidth and computation and that the number of a participant's neighbors that lie along the path of that participant's particular client may be too small to make this procedure effective.

$ProofOfShipment(x, b, 1)$ where the single node that is responsible for providing a proof of shipment is the next node on the path contract who can provide proof of receipts, can be used by entity x to provide proof of shipment of a batch b. In cases the next node on the path does not cooperate, that node and its preceding node are localized. Also, when a participant lies about forwarding a message, this participant and the next node downstream are localized. In order to for $ProofOfShipment$ to be functional there must exist a trusted channel between the entity that is providing a proof and the verifier. This is an issue that is not addressed in [3, 5] (see Section A.2 for examples of attacks), but that we address by assuming a trusted between each entity and the CM.

A security weakness of $ProofOfShipment$ procedure in link-level accountability settings stems from nodes having a possibility of issuing false proofs of receipt. For example, when destination d is not trusted, to get paid ϵ_d d may wish to provide acknowledgment even to batches it did not receive. A possible solution to this issue is to adopt a secure procedure for proving receipt of shipment (e. g. secure summarization [12]). Also, in order to prevent forwarding nodes from not issuing acknowledgments of receipt altogether, a rule that no node can get paid for a forwarded message unless it provides both proof of receipt and proof of shipment (proof of receipt from the next node downstream) of that message can be adopted. The latter is a rephrasing of the 2.3.1 which is mentioned explicitly in Section 2.3.1.

A.2 Vulnerability of Schemes Presented in [5, 16] With Respect to Multiple Independent Adversaries

The accountability scheme presented by Laskowski and Chuang in [16] assumes a single adversary. At a very high level, it works by having a trusted contractual monitor on each node of a path in order to make sure that nodes only forward traffic to hops that meet certain optimality constraints agreed upon in advance. At the beginning, the source is promised by its service provider connectivity to certain destinations at certain optimality level, that source's service provider is promised a similar deal from its own service provider, and so on and so forth. When the source's traffic is treated with suboptimal quality, which can be detected with aid of trusted contractual monitors, the source penalizes its service provider. The latter in turn penalizes its service provider, and so on and so forth until this penalty wave reaches the faulty node. At this point the latter node cannot penalize any one down stream, so it must incur losses due to its deviation from contractual agreements. When the only obligation of service providers is to route traffic towards the next hop on the most optimal route, this scheme works assuming that traffic does not come back from a suboptimal path to an optimal path before it reaches the destination. In presence of multiple adversaries who may intentionally delay or add jitter to traffic, however, only the adversary closest to the source will be punished as there is no mechanism for propagating penalties beyond this point for such type of malicious behavior.

At a high level, the scheme presented in [5] by Barak et al. works as follows. Each node on a path forms a quality of service report and sends it to the source in an onion fashion. If reports of two adjacent nodes disagree, a faulty link is localized. The nature of the onion report ensures that an adversary cannot implicate any particular participant by dropping a report. However, in presence of multiple adversaries, it is enough for one adversary to drop these onion reports in order for the source to have no knowledge regarding any other adversary and the quality of the path down stream from the one who drops onion reports. For path-based contract systems such a simple attack makes it hard for the source to decide whether the nodes down stream from the adversary who drops the reports should get paid or penalized.

B. Analysis of Path-Segment Contract System with Node-Level Accountability and Proofs from Sections 3.2- 3.3

B.1 Success of Path-Segment Contracts with Node-Level Accountability and Proportional Payments

In the case that the CM has capability of correctly determining the precise amount of parts that each forwarding node forwards for every round of the game, node-level accountability is guaranteed. In this setting the CM is capable of determining whether a forwarding node is faulty or not, for every forwarding node in the game, and administer payment or punishment accordingly. If an agreement is reached, in the negotiations stage s must make a commitment C_i to each node n_i, and, as noted in Section 5, C_i should equal to $mc_i \frac{t_i}{N}$. This commitment assumes that n_i at least meets its threshold, but s must agree to pay $\frac{c_i}{N}$ for each extra part that n_i forwards beyond t_i. Expected profit equation of forwarding node n_i is:

$$\mathrm{E}[\pi_{n_i}] = mc_i\frac{t_i}{N} + \xi_{i_1}c_i - \xi_{i_2}f_i - \xi_{i_3}p_i,$$

$$\text{where } \xi_{i_1} = \frac{m}{N}\left[\sum_{\varphi_i=t_i}^{N}\sigma_i(\varphi_i|\varphi_{i-1}\geq t_{i-1})(\varphi_i - t_i)\right],$$

$$\xi_{i_2} = \frac{m}{N}\left[\sum_{\varphi_i=t_i}^{N}\sigma_i(\varphi_i|\varphi_{i-1}\geq t_{i-1})\varphi_i\right], \text{ and}$$

$$\xi_{i_3} = m\sigma_i(0|\varphi_{i-1}\geq t_{i-1}).$$

This equation is the difference between what n_i is expected to earn by exceeding t_i when n_{i+1} acknowledges n_is forwarding actions during forwarding stage in addition to what n_i gains from ss commitment to n_is bandwidth in the negotiations stage and n_is expected marginal forwarding costs in addition to expected penalties when n_i is unable to prove that it meets contractual obligations. For each forwarding node n_i the optimal distribution σ_i should maximize ξ_{i_1} and ξ_{i_2}, by forwarding every packet received from n_{i-1} such that $\xi_{i_1} = \sum_{\varphi_i=t_{i-1}}^{N}\sigma_{i-1}(\varphi_{i-1}=\varphi_i)(\varphi_i - t_i)$, and make sure that $\xi_{i_3} = 0$ when $\frac{t_i}{N}[c_i - f_i] + p_i > 0$ and vice versa. Also, in the former case, for n_i to make money c_i must be greater than f_i.

Expected profit equation of source s is:

$$\mathrm{E}[\pi_s] = \sigma_\ell(\varphi_\ell \geq t)\sum_{i=1}^{m}u_i - \sum_{j=1}^{\ell}\left[\xi_{j_1}c_j + mc_j\frac{t_j}{N}\right] + \sum_{j=1}^{\ell}\xi_{j_2}p_j.$$

This equation is the difference between what s is expected to earn from penalties of forwarding nodes in $P_{s\to d}$ when they are unable to prove that they meet contractual obligations in addition to the expected overall utility of batches in b reaching d and what s is expected to pay to all forwarding nodes s has Path-Segment contract with when they exceed their respective thresholds in addition to ss commitment to their bandwidth. In the case that every n_i meets t_i for every batch in b, the optimal values of σ_0 are 1 when $\sum_{i=1}^{m}u_i \geq \epsilon_s + \sum_{j=1}^{\ell}(\xi_{j_1}c_j + mc_j\frac{t_j}{N})$ and 0 otherwise. The total system profit in this scenario is at most $\sum_{i=1}^{m}u_i - m\sum_{i=1}^{\ell}\frac{t_i}{N}f_i$ when $\sigma_0 = 1$ and 0 otherwise. Say at least one forwarding node found that it is best for it not to meet its threshold; without loss of generality let us say that the faulty node closest to s is n_i. The optimal value of σ_0 is 1 when

$$mp_i \geq \sum_{j=1}^{i-1}\xi_{j_1}c_j + m\sum_{j=1}^{\ell}c_j\frac{t_j}{N} + \epsilon_s$$

and 0 otherwise. In this situation the total system profit is 0 regardless of the value of σ_0.

LEMMA 4. *If $\sum_{i=1}^{m}u_i \geq \epsilon_s + \sum_{i=1}^{\ell}\epsilon_i + m\sum_{i=1}^{\ell}f_i$, then there is a bandwidth price setting $\mathbf{c} = \langle c_1, c_2, ..., c_\ell\rangle$ that yields an equilibrium where at least t parts of all m batches reach d in the expected case and s as well as each node on the path excluding d makes a positive profit no less than its corresponding minimum settlement.*

Proof. : $\sum_{i=1}^{m}u_i \geq \epsilon_s + \sum_{i=1}^{\ell}\epsilon_i + m\sum_{i=1}^{\ell}f_i$ implies that we can find a price vector $\mathbf{c} = \langle c_1, c_2, ..., c_\ell\rangle$ such that $\sum_{i=1}^{m}u_i \geq \epsilon_s + m\sum_{i=1}^{\ell}c_i$ and $c_i \geq f_i + \epsilon_{n_i}\ \ \forall\, 1 \leq i \leq \ell$ e.g.

$$c_i = f_i + \frac{\epsilon_{n_i}}{m} + \frac{\sum_{i=1}^{m}u_i - \sum_{i=0}^{\ell}\epsilon_i - m\sum_{i=1}^{\ell}f_i}{m(\ell+1)}.$$

If every forwarding node meets its threshold, this yields an overall positive profit for s, d and every forwarding node n_i no less than their respective minimum settlement in addition to $\frac{\sum_{i=1}^{m}u_i - \sum_{i=0}^{\ell}\epsilon_i - m\sum_{i=1}^{\ell}f_i}{\ell+1}$. Thus, the condition $c_i > f_i$ holds $\forall 1 \leq i \leq \ell$ and every forwarding node n_i will try to forward every part of every batch that s sends so s will send every batch in b. Since even in the worst case of general network failures such as congestion each node should be able to meet its corresponding threshold by Assumption 1, at least t parts should reach d in the expected case. ■

THEOREM B.1. *Path-Segment contract systems meet definition of successful mechanism design with node-level accountability and proportional payments.*

Proof.

Provided that a node-level accountability framework effective against multiple independent adversaries is established and that penalties are high enough to cover all of s's aggregate expected contractual spending in addition to ϵ_s (see Sections 3.1 and 4.2), Lemma 4 shows that Path-Segment contract systems satisfy success definition for contract systems with link-level accountability for proportional payments.

■

To show that Path-Segment contract systems satisfy success definition for contract systems with node-level accountability and all-or-nothing payments the same logic as the proof of Theorem 3.1 can be used.

B.2 Proof of Lemma 1

Proof. When d is trusted or encouraged to acknowledge everything that n_ℓ forwards and $c_\ell > f_\ell$, n_ℓ will be discouraged from not meeting its threshold $t_\ell = t$. Similar argument follows for the rest of the nodes by using backward induction, where n_ℓ is the base case, keeping in mind that each node n_i will be discouraged from not meeting its corresponding threshold. The latter is true because every node n_i is encouraged to forward everything that n_i receives since its payoff is directly proportional to the number of parts it forwards. $\sum_{i=1}^{m}u_i \geq \sum_{i=0}^{\ell+1}\epsilon_i + m\sum_{i=1}^{\ell}f_i$ implies that we can find a price vector $\mathbf{c} = \langle c_1, c_2, ..., c_\ell\rangle$ such that

$\sum_{i=1}^{m} u_i \geq \epsilon_s + \epsilon_d + m\sum_{i=1}^{\ell} c_i$ and $c_i \geq f_i + \epsilon_{n_i}\ \forall\, 1 \leq i \leq \ell$ e.g.

$$c_i = f_i + \frac{\epsilon_{n_i}}{m} + \frac{\sum_{i=1}^{m} u_i - \sum_{i=0}^{\ell+1} \epsilon_i - m\sum_{i=1}^{\ell} f_i}{m(\ell+2)}.$$

If every forwarding node meets its threshold, this yields an overall positive profit for s, d and every forwarding node n_i no less than their respective minimum settlement in addition to $\frac{\sum_{i=1}^{m} u_i - \sum_{i=0}^{\ell+1} \epsilon_i - m\sum_{i=1}^{\ell} f_i}{\ell+2}$. Thus, every forwarding node n_i will try to forward every part of every batch that s sends and s will send every batch in b. Since even in the worst case of general network failures such as congestion each node should be able to meet its corresponding threshold by Assumption 1 (unintentional drops), at least t parts should reach d in the expected case. ■

Proof. [Proof of Theorem 3.1]. Provided that a link-level accountability framework effective against multiple independent adversaries is established and that penalties are high enough to cover all of s's aggregate expected contractual spending in addition to ϵ_s (see Sections 3.1 and 4.2), Lemma 1 shows that Path-Segment contract systems satisfy success definition for contract systems with link-level accountability and proportional payments. ■

B.3 Proof of Lemma 2

Proof. When d is encouraged to acknowledge everything that n_ℓ forwards and $c_\ell > f_\ell$, n_ℓ will be discouraged from not meeting its threshold $t_\ell = t$. The last node n_ℓ is also discouraged from forwarding more than t parts to d because such strategy will result in higher forwarding cost while yielding the same reward as for forwarding only t parts. Similar argument follows for the rest of the nodes using inverse induction. However, every node is interested in sending as little as possible in order to reduce forwarding cost. Since $p_{i_a} < p_{i_b}$ for every node n_i, when cheating, no node n_i wants to be blamed for not receiving at least t_{i-1} packets; n_i loses less when it is able to blame the next node downstream which n_i can do only if n_i can prove that it received at least t_{i-1} parts, according to 2.3.1 (see Section 2.3.1). Therefore, if every node meets its threshold it is guaranteed to get paid $\frac{t_i}{N}c_i$. However, if $\sigma_\ell(\varphi_\ell \geq t | t \leq \varphi_i < t_i) = 1$, then it does not make sense for n_i to meet its threshold as it is guaranteed to get paid while decreasing its marginal forward costs. By Assumption 1, every node n_i has a non-trivial probability of unintentionally dropping $t_i - t_{i-1}$ packets due to general network failures such as congestion, which means that there must be non-trivial probability that every node n_i unintentionally drops $t_i - t_{i-1}$ packets of a specific message. This implies that there is non-trivial probability that more than $N - t$ packets of a message get dropped if at least one node does not meet its threshold. Therefore, $\sigma_\ell(\varphi_\ell \geq t|\varphi_i) < 1\ \forall\, t \leq \varphi_i < t_i$ holds $\forall\, 1 \leq i \leq \ell$, and in order to encourage n_i to meet t_i it must be the case that:

$$\frac{t_i}{N}[c_i - f_i] > \sigma_\ell(\varphi_\ell \geq t | t \leq \varphi_i < t_i)\frac{t_i}{N}c_i -$$

$$\sigma_\ell(\varphi_\ell < t | t \leq \varphi_i < t_i)p_{i_a} - \varphi_i\frac{f_i}{N},$$

which can be rewritten as

$$c_i\frac{t_i}{N}[1 - \sigma_\ell(\varphi_\ell \geq t | t \leq \varphi_i < t_i) + \sigma_\ell(\varphi_\ell < t | t \leq \varphi_i < t_i)\varepsilon_i] >$$

$$(t_i - \varphi_i)\frac{f_i}{N}.$$

where $\varepsilon_i = \frac{Np_{i_a}}{t_i c_i}$ and $\varphi_i < t_i$. Note that this equation cannot be satisfied if $\sigma_\ell(\varphi_\ell \geq t | t \leq \varphi_i < t_i) = 1$. Since $\sum_{i=1}^{m} u_i > m\sum_{i=1}^{\ell} f_i$, we know from the proof of Lemma 1 that we can find $c_i > f_i$ for every forwarding node n_i (assuming non-zero minimum settlements for each node). Therefore, it is sufficient to have

$$\frac{\varphi_i}{t_i} \geq \sigma_\ell(\varphi_\ell \geq t|\varphi_i) - \sigma_\ell(\varphi_\ell < t|\varphi_i)\varepsilon_i\ \ \forall\, t \leq \varphi_i < t_i$$

or

$$p_{i_a} \geq \left[\frac{\sigma_\ell(\varphi_\ell \geq t|\varphi_i) - \frac{\varphi_i}{t_i}}{\sigma_\ell(\varphi_\ell < t|\varphi_i)}\right]\frac{t_i}{N}c_i,\ \forall\, t \leq \varphi_i < t_i.$$

The CM can ensure that this condition is met by increasing p_{i_a}. When this condition is met, min('1', '2', '3') is '1' and every node n_i will be willing meet t_i exactly. Therefore s will send every batch in b, and exactly t parts of every batch in b will make it to d. Computation of the profit of each forwarding node including d is the same as in the proof of the previous claim. Since penalties are distributed only when $\varphi_\ell < t$, the CM has to perform only a single check every round to make sure that d receives at least t parts of every batch. The CM's direct manipulation of p_{i_a} may not be necessary when $\sigma_\ell(\varphi_\ell \geq t|\varphi_i)$ is low and the latter is reasonable to assume considering that all forwarding nodes are selfish and do not trust each other. ■

Proof. [Proof of Theorem 3.2] Is analogous to the proof of Theorem 3.1 ■

B.4 Proof of Lemma 3

Proof. If such requirement was not necessary, then there must exist at least one solution to contractual failure when connectivity is purchased for at least two distinct flows at one price without making these flows distinguishable. However, as the examples in Section 3.3 show, even with only as many as two flows depeering may occur when entities are unable to negotiate bandwidth costs per flow.

Prior to showing why this requirement is sufficient in general, let us first show why it is sufficient for the examples described in Section sec:PairwiseFail. In the first example if every node could negotiate contracts per each flow, then no estimation would be necessary because every node will have negotiated the exact rate at which traffic will be sent for each flow. In the second example, as long as each source can negotiate contracts with X on per-flow basis s_1 will have chosen to pay for 1 unit only to D_1 and $s_{1<i\leq n}$ will have chosen to pay for 1 unit each only to D_2. No depeering will take place and X will have made a positive profit of nc_x.

Before going any further we note that for a forwarding node n_i to request a proof of shipment from n_{i+1} of a batch for a particular flow, prior establishment of a Pairwise-Exchange contract between n_i and n_{i+1} for that specific flow is necessary.

For the sake of contradiction say that each node is required to negotiate Pairwise-Exchange contracts at per-flow granularity, there is an available flow path $P_{s\to d}$, and s has enough funds to pay each node along $P_{s\to d}$ at least that node's minimum settlement in addition to that node's forwarding cost, but s is unable to reach d because n_i and n_{i+1} decide to depeer. We will consider this decision from n_i's point of view. For n_i exchanging flows may be unprofitable when either (i) n_i is unable to meet $\sum_{j=i+1}^{\ell} f_j + \epsilon_j$ or (ii) n_{i+1} is asking n_i for more than $\sum_{j=i+1}^{\ell} f_j + \epsilon_j$. In the scenario (i), it must be the case that n_{i-1} cannot meet $\sum_{j=i}^{\ell} f_j + \epsilon_j$, which in turn implies that n_{i-2} cannot meet $\sum_{j=i-1}^{\ell} f_j + \epsilon_j$, and so on until the implication that s is unable to meet $\sum_{j=1}^{\ell} f_j + \epsilon_j$ is reached. Thus scenario (i) leads to a contradiction. In the scenario (ii), asking for too much from n_i, n_{i+1} ends up making no profit, whereas it could make at least $\epsilon_{n_{i+1}}$ were n_{i+1} to ask for no more than $\sum_{j=i+1}^{\ell} f_j + \epsilon_j$. Thus case (ii) contradicts the assumption that every participant is rational. ■

B.5 Proof of Theorem 3.3

Proof.

Let us begin this proof by showing why Pairwise-Exchange contract systems that require negotiation at per-flow granularity meet the last part of the definition of successful mechanism design with link-level accountability and proportional payments. When an agreement is reached in the negotiations stage, s makes a commitment of $C_1 = mc_1\frac{t_1}{N}$ to the first forwarding node on $P_{s\to d}$, and s pays $\frac{c_1}{N}$ for each extra part that n_1 forwards beyond t_1. Similarly, every forwarding node $n_i\ \forall\ 1 \leq i \leq \ell - 1$ makes a commitment of $C_{i+1} = mc_{i+1}\frac{t_{i+1}}{N}$ to the next node on $P_{s\to d}$, and n_i pays $n_{i+1}\ \frac{c_1}{N}$ for each extra part that n_{i+1} forwards beyond t_{i+1}. Thus, the expected profit of a forwarding node n_i is:

$$\begin{aligned}
\mathrm{E}[\pi_{n_i}] &= [\text{forwarding gains}] - [\text{bandwidth costs}] - \\
&\quad [\text{forwarding \& penalty losses}] \\
&= \left[mc_i\frac{t_i}{N} + \xi_{i_1}\cdot c_i\right] - \left[mc_{i+1}\frac{t_{i+1}}{N} + \xi_{(i+1)_1}\cdot c_{i+1}\right] \\
&\quad -[\xi_{i_2}\cdot f_i\ + \xi_{i_3}\cdot p_{i_a} + \\
&\quad \sigma_i(0|\varphi_{i-1}\geq t_{i-1})[\lambda_{i_a}(\varphi_i \geq t_i)p_{i_a} + \\
&\quad \lambda_{i_b}(\varphi_{i-1} < t_{i-1})p_{i_b}] + \\
&\quad \sigma_{i-1}(0)\lambda_{(i-1)_a}(\varphi_{i-1}\geq t_{i-1})p_{i_b}],
\end{aligned}$$

$$\begin{aligned}
\text{where}\quad \xi_{i_1} &= \frac{m}{N}\sum_{\varphi_i=t_i}^{N}\lambda_{(i+1)_b}(\varphi_i)(\varphi_i - t_i), \\
\xi_{i_2} &= \frac{m}{N}\sum_{\varphi_i=t_i}^{N}\sigma_i(\varphi_i)\varphi_i, \\
\text{and}\quad \xi_{i_3} &= m\left[\sum_{\varphi_i=t_i}^{N}\sigma_i(\varphi_i)\right]\lambda_{(i+1)_b}(0).
\end{aligned}$$

Here $\xi_{(i+1)_1}$ is defined analogously to ξ_{i_1}. This equation is exactly the same as the one for Path-Segment contract systems with the exception that each forwarding node n_i must also pay to n_{i+1} for connectivity. Sufficient condition for n_i to forward traffic and make positive profit is for the expected gains that n_i makes from properly forwarding n_{i-1}^{th} traffic to be larger than the losses it may incur due to penalties, its own forwarding costs, and what n_i has to pay n_{i+1}. Just as for the Path-Segment scenario, an important aspect of $\mathrm{E}[\pi_{n_i}]$ is that the profit of n_i depends on the strategies of its neighbors. There is nothing n_i can do if n_{i-1} lies about forwarding at least t_{i-1} parts, and if n_i does not have any confidence in n_{i+1}, then n_i would forward nothing to prevent fruitless forwarding costs. Therefore, sufficient incentive mechanism must provide n_i with confidence in its neighbors, specifically for n_i to be sure that n_{i+1} acknowledges everything that n_i forwards to n_{i+1}.

Say t is the expected amount of parts of any batch in b that $P_{s\to d}$ can deliver from s to d, given that s sends out N parts. The expected profit of the source s is:

$$\begin{aligned}
\mathrm{E}[\pi_s] &= [\text{utility}] - [\text{bandwidth costs}] + [\text{penalties}] \\
&= \left[\sigma_\ell(\varphi_\ell \geq t)\sum_{i=1}^{m} u_i\right] - \left[mc_1\frac{t_i}{N} + \xi_{1_1}c_1\right] + \\
&\quad m\sigma_1(0|\varphi_0 = N)p_{1_1}.
\end{aligned}$$

This equation is exactly the same as the one for Path-Segment contract systems with the exception that s pays to and is able to obtain penalties from only n_1 (see details on penalties in Section 4.2). If s has high confidence in that $\varphi_\ell \geq t$, then it is sufficient for $\sum_{i=1}^{m} u_i \geq \epsilon_s + \xi_{1_1}c_1 + mc_1\frac{t_1}{N}$ for s to have incentive to send traffic via reimbursements. If s has no confidence in that $\varphi_\ell \geq t$, if at least one forwarding node n_j found that it is best for it not to forward, then there is nothing s can do unless $j = 1$

in which case s can send traffic and make money only if $mc_1\frac{t_i}{N} + \xi_{1_1}c_1 < mp_{i_a}$.

To ensure that s can make positive profit, the CM must enforce penalties to be higher than all of s's expected marginal costs over the whole path $P_{s\to d}$ (see Section 4.2 for further detail), which means that every node's penalty must be at least its forwarding cost. This condition ensures that for no node will it be profitable to advertise bandwidth it does not have, assuming that no forwarding node n_i will agree to a bandwidth cost c_i lower than its forwarding cost f_i. If we assume that s is trusted, then p_{i_a} should be higher than all of s's expected marginal costs.

Equation for $\mathrm{E}[\pi_s]$ shows that it might be profitable for s to to send less than its threshold towards d in case $\sigma_\ell(\varphi_\ell > t|\varphi_0 < N)$ is consistently close to 1. While obtaining only a constant utility u_j for each batch $b_j \in b$ when at least t parts of b_j reach d, s must pay n_1 extra for each part of b_j that n_1 forwards in excess of t_1 parts. However, by the Claiming Shipment Rule (see Section 2.3.1) in this scenario n_1 would not be able to get paid which would cause it to drop every batch to prevent fruitless forwarding costs. From penalties, s would not be able to profit at least its minimum settlement ϵ_s due to the structure of penalties as presented in Section 4.2. Therefore, being rational, s would rather send out exactly N parts for each batch.

The following claim shows that Pairwise-Exchange contract systems that require negotiation at per-flow granularity meet the last part of the definition of successful mechanism design with link-level accountability and proportional payments.

Claim: For Pairwise-Exchange contract systems that require negotiation at per flow granularity, if d is trusted or encouraged with payment $\frac{\epsilon_d}{m}$ to acknowledge receipt of φ_ℓ parts from n_ℓ, this information is known to every participant, $\sum_{i=1}^{m} u_i \geq \sum_{i=0}^{\ell+1}\epsilon_i + m\sum_{i=1}^{\ell} f_i$, and $c_i - f_i \geq c_{i+1} + \epsilon_{n_i}\ \ \forall\, 1 \leq i \leq \ell$, then there is an equilibrium bandwidth price setting $\mathbf{c} = \langle c_1, c_2, ..., c_\ell\rangle$ such that t parts of every batch in b reach d in the expected case, and each element of $P_{s\to d}$ makes a positive profit no less than its respective minimum settlement.

Proof of Claim:

When d is trusted or encouraged to acknowledge everything that n_ℓ forwards and $c_\ell > f_\ell$, n_ℓ will be discouraged from not meeting its threshold $t_\ell = t$. Similar argument follows for the rest of the nodes by using backward induction, where n_ℓ is the base case, keeping in mind that each node n_i will be discouraged from not meeting its corresponding threshold. The latter is true because every node n_i is encouraged to forward everything that n_i receives since its payoff is directly proportional to the number of parts it forwards. $\sum_{i=1}^{m} u_i \geq \sum_{i=0}^{\ell+1}\epsilon_i + m\sum_{i=1}^{\ell} f_i$ implies that negotiations can result in a bandwidth-cost vector $\mathbf{c} = \langle c_1, c_2, ..., c_\ell\rangle$ such that $\sum_{i=1}^{m} u_i \geq \epsilon_s + \epsilon_d + m\sum_{i=1}^{\ell} c_i$ and $c_i \geq f_i + \epsilon_{n_i}\ \ \forall\, 1 \leq i \leq \ell$ e.g.

$$c_i = f_i + \frac{\epsilon_{n_i}}{m} + \frac{\sum_{i=1}^{m} u_i - \sum_{i=0}^{\ell+1}\epsilon_i - m\sum_{i=1}^{\ell} f_i}{m(\ell+2)}.$$

This can be achieved during the negotiations as follows. First, s establishes a Pairwise-Exchange contract with n_1 to forward s's traffic towards d. The most n_1 can bargain out of s is $\sum_1^m u_i - \epsilon_s \geq m\sum_{i=1}^{\ell} f_i + \sum_{i=1}^{\ell+1}\epsilon_i$. Second, in order to forward s's traffic properly, n_1 establishes a Pairwise-Exchange contract with n_2 to forward s's traffic towards d. The most n_2 can bargain out of n_1 is $\sum_{i=1}^{m} u_i - \epsilon_s - f_1 - \epsilon_{n_1} \geq m\sum_{i=2}^{\ell} f_i + \sum_{i=2}^{\ell+1}\epsilon_i$. This goes on until n_ℓ is reached who has to bargain with d to obtain acknowledgments. The most n_ℓ can bargain out of $n_{\ell-1}$ for forwarding s's traffic is $\sum_{i=1}^{m} u_i - m\sum_{i=1}^{\ell-1} f_i - \sum_{i=0}^{\ell-1}\epsilon_i \geq f_\ell + \epsilon_{n_\ell} + \epsilon_d$. Thus, n_ℓ will have enough funds to bargain with d acknowledgments. Note that s pays every node along $P_{s\to d}$ by paying n_1. If every forwarding node meets its threshold, this yields an overall positive profit for s, d and every forwarding node n_i no less than their respective minimum settlement in addition to $\frac{\sum_{i=1}^{m} u_i - \sum_{i=0}^{\ell+1}\epsilon_i - m\sum_{i=1}^{\ell} f_i}{\ell+2}$. Thus, every forwarding node n_i will try to forward every part of every batch that s sends, s will send N parts of every batch in b, and the expected amount of parts t of every batch in b will reach d. ■

Provided that a link-level accountability framework is effective against multiple independent adversaries is established and that penalties are more than needed to cover all of s's aggregate expected contractual spending (see Sections 3.1 and 4.2), this claim shows that Pairwise-Exchange contract systems with the requirement to negotiate contracts at per-flow granularity satisfy definition of successful mechanism design with link-level accountability and proportional payments.

■

B.6 Proof of Theorem 3.4

Proof. This requirement is necessary, because without it there is no way for the CM to check quality of an overall path, and, since the CM is the only entity with authority to check proofs of receipt, it is the CM who must monitor overall path quality. To begin the proof of why this condition is sufficient, we note that simply if the CM has a record of each flow, then for each flow path it can check how many parts per round a destination of that flow path obtains and act according to whether it meets the overall path threshold. The latter, s has no control over, and the CM must measure this quantity separately for each flow.

We begin a more detailed treatment of the proof by showing why Pairwise-Exchange contract systems that require negotiation at per-flow granularity and require CM to monitor the overall quality level of paths, meet the last part of the definition of successful mechanism design with link-level accountability and all-or-nothing payments. When an agreement is reached in the negotiations stage, s makes a commitment of $C_1 = mc_1\frac{t_1}{N}$ to the first forwarding node on $P_{s\to d}$, and every forwarding node $n_i\ \forall\, 1 \leq i \leq \ell - 1$ makes a commitment of $C_{i+1} = mc_{i+1}\frac{t_{i+1}}{N}$ to the next node on $P_{s\to d}$. As long as $\varphi_\ell \geq t$, every node n_i gets paid a fixed bandwidth cost $c_i\frac{ti}{N}$, otherwise each node n_i has to prove that it

met its threshold t_i in order to get paid. Say t is the amount of parts of any batch in b that $P_{s\to d}$ can deliver from s to d when all forwarding nodes cooperate, given that s sends out N parts. The expected profit of a forwarding node n_i is:

$$\begin{aligned}\mathrm{E}[\pi_{n_i}] &= [\text{forwarding gains}] - [\text{bandwidth costs}] - \\ &\quad [\text{forwarding \& penalty losses}] \\ &= \left[mc_i\frac{t_i}{N}\right] - \left[mc_{i+1}\frac{t_{i+1}}{N}\right] - [\xi_{i_1} + \xi_{i_2} + \\ &\quad m\sigma_i(0|\varphi_{i-1} \geq t_{i-1})[\lambda_{i_a}(\varphi_i \geq t_i)\cdot \\ &\quad p_{i_a} + \lambda_{i_b}(\varphi_{i-1} < t_{i-1})p_{i_b}] + \\ &\quad m\sigma_{i-1}(\varphi_{i-1} < t_{i-1})\lambda_{(i-1)_a}(\varphi_{i-1} \geq t_{i-1})p_{i_b}],\end{aligned}$$

$$\begin{aligned}\text{where}\quad \xi_{i_1} &= m\sum_{\varphi_i=t_i}^{N}\sigma_i(\varphi_i)\left(\frac{\varphi_i}{N}f_i + \lambda_{(i+1)_b}(\varphi_i < t_i)p_{i_a}\right)\cdot \\ &\quad (1 - \sum_{\varphi_{i+1}=t}^{\varphi_i}\binom{\varphi_i}{\varphi_{i+1}}\sigma_{i+1}(\varphi_{i+1})\,[\cdots] \\ &\quad \left[\cdots\left[\sum_{\varphi_\ell=t}^{\varphi_{\ell-1}}\binom{\varphi_{\ell-1}}{\varphi_\ell}\sigma_\ell(\varphi_\ell)\right]\cdots\right]),\end{aligned}$$

$$\begin{aligned}\text{and}\quad \xi_{i_2} &= m\sum_{\varphi_i=t}^{t_i-1}\sigma_i(\varphi_i)(\lambda_{i_a}(\varphi_i \geq t_i)p_{i_a} + \\ &\quad \lambda_{i_b}(\varphi_{i-1} < t_{i-1})p_{i_b} + \frac{\varphi_i}{N}f_i)\cdot \\ &\quad (1 - \sum_{\varphi_{i+1}=t}^{\varphi_i}\binom{\varphi_i}{\varphi_{i+1}}\sigma_{i+1}(\varphi_{i+1})\,[\cdots] \\ &\quad \left[\cdots\left[\sum_{\varphi_\ell=t}^{\varphi_{\ell-1}}\binom{\varphi_{\ell-1}}{\varphi_\ell}\sigma_\ell(\varphi_\ell)\right]\cdots\right]).\end{aligned}$$

Note the use of Assumption 2 (independence) for profit analysis. This equation is very similar to the one for proportional payments; the differences are that n_i's gain is fixed to the commitment that was made to it by n_{i-1} and n_i's bandwidth cost to n_{i+1} is also fixed. Sufficient condition for n_i to forward traffic and make positive profit is for the expected gains that n_i makes from properly forwarding n_{i-1}^{th} traffic to be larger than the losses it may incur due to penalties, its own forwarding costs, and what n_i has to pay n_{i+1}. Node's losses due to penalties depend on whether the final node n_ℓ meets its threshold t, so besides n_i's confidence in its neighbors, n_i's confidence in whether $\sigma_\ell(\varphi_\ell > t)$ is high is important. If $\sigma_\ell(\varphi_\ell > t)$ is high, n_i may be encouraged to forward $t \leq \varphi_i \leq t_i$ in order to prevent extra losses due to forwarding. Therefore, sufficient incentive mechanism must provide n_i with confidence in its neighbors and make it unprofitable to economize on forwarding costs.

Expected profit equation of s is:

$$\begin{aligned}\mathrm{E}[\pi_s] &= [\text{utility}] - [\text{bandwidth costs}] + [\text{penalties}] \\ &= \left[\sigma_\ell(\varphi_\ell \geq t)\sum_{i=1}^{m}u_i\right] - \left[mc_1\frac{t_i}{N}\right] + \\ &\quad m\sigma_1(0|\varphi_0 = N)p_{1_1}.\end{aligned}$$

The main difference between this equation and that of source's profit in the proportional payments case is that in the case of all-or-nothing payments the source does not have to pay to forwarding nodes more than the commitment and failure is addressed only when n_ℓ does not meet t. If s has high confidence in that $\varphi_\ell \geq t$, then it is sufficient for $\sum_{i=1}^{m}u_i \geq \epsilon_s + mc_1\frac{t_j}{N}$ for s to send traffic and make positive profit. If s has no confidence in that $\varphi_\ell \geq t$, and if at least one forwarding node n_j found that it is best for it not to forward, then there is nothing s can do unless $j = 1$, in which case s can still have incentive to send traffic via reimbursement if $mc_1\frac{t_i}{N} + \xi_{1_1}c_1 < mp_{i_a}$. Just as for the scenario with proportional payments, to ensure that s can make positive profit, the CM must enforce penalties to be higher than all of s's expected marginal costs over the whole path $P_{s\to d}$ (see Section 4.2 for further detail), which means that every node's penalty must be at least that node's forwarding cost. This condition ensures that for no node will it be profitable to advertise bandwidth it does not have, assuming that no forwarding node n_i will agree to a bandwidth cost c_i lower than its forwarding cost f_i. If we assume that s is trusted, then p_{i_a} should be higher than all of s's expected marginal costs.

Claim: For Pairwise-Exchange contract systems that require negotiation at per flow granularity and the CM to monitor the overall path quality level, if d is trusted or encouraged with payment $\frac{\epsilon_d}{m}$ to acknowledge receipt of φ_ℓ parts from n_ℓ, this information is known to every participant, $\sum_{i=1}^{m}u_i \geq \sum_{i=0}^{\ell+1}\epsilon_i + m\sum_{i=1}^{\ell}f_i$, and $c_i - f_i \geq c_{i+1} + \epsilon_{n_i}\ \ \forall\ 1 \leq i \leq \ell$, then there is an equilibrium bandwidth price setting $\mathbf{c} = \langle c_1, c_2, ..., c_\ell\rangle$ such that exactly t parts of every batch in b reach d in the expected case, and each element of $P_{s\to d}$ makes a positive profit no less than its respective minimum settlement.

Proof of Claim (sketch): It was already shown that the requirement for Pairwise-Exchange contacts to be established per flow is sufficient for Pairwise-Exchange contract systems to meet success definition with link-level accountability and proportional payments. The proof of this claim given the modification that the CM can monitor quality of each flow path is analogous to proof of Lemma 2 keeping in mind that d must be encouraged to provide proof of receipt of batches from n_ℓ, $p_{i_a} < p_{i_b}$ must hold (and it does by default because of the way penalties are structured in Pairwise-Exchange contracts as discussed in Section 4.2), and the necessary utility and price conditions, $\sum_{j=1}^{m}u_i > mc_1 + \epsilon_s$ and $c_i - f_i \geq c_{i+1} + \epsilon_{n_i}\ \ \forall\ 1 \leq i \leq \ell - 1$ respectively, must be met as mentioned in Section 3.3. ■

Provided that a link-level accountability framework is effective against multiple independent adversaries is established and that penalties are more than needed to cover all

of s's aggregate expected contractual spending (see Sections 3.1 and 4.2), this claim shows that Pairwise-Exchange contract systems with the requirements to negotiate contracts at per-flow granularity and for the CM to monitor overall path quality satisfy definition of successful mechanism design with link-level accountability and all-or-nothing payments.

■